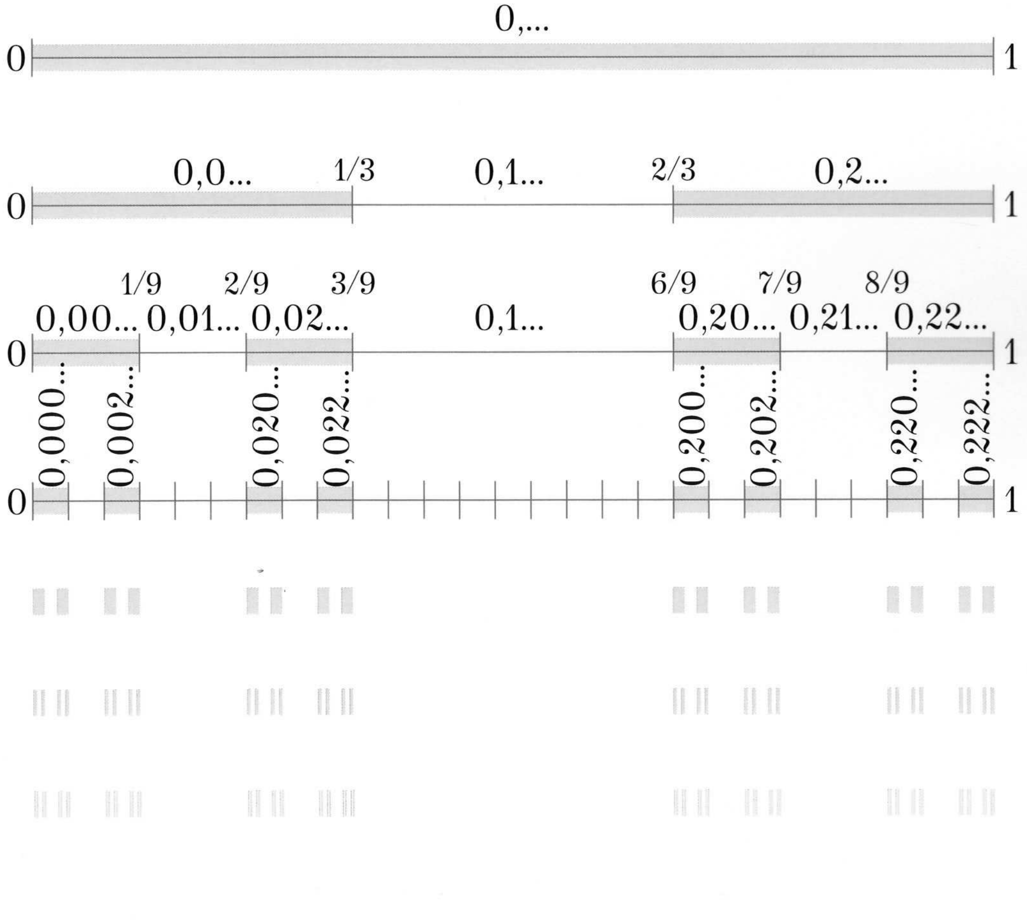
Небојша Икодиновић

УВОД У МАТЕМАТИЧКУ ЛОГИКУ



Математички факултет

У[illegible]

Универзитет у Београду – Математички факултет

УВОД У МАТЕМАТИЧКУ ЛОГИКУ

Небојша Икодиновић

Београд, 2023

др Небојша Икодиновић

УВОД У МАТЕМАТИЧКУ ЛОГИКУ
Прво издање, 2023

Рецензенти:
др Предраг Тановић, научни саветник Математичког института САНУ
др Славко Моцоња, доцент Математичког факултета, Универзитет у Београду

Издавач: Универзитет у Београду – Математички факултет
Студентски трг 16, 11158 Београд, тел. (+381) 011 2027 801, matf@matf.bg.ac.rs

За издавача: др Зоран Ракић, декан

Обрада текста: аутор
Цртежи и корице: аутор
Фотографије: `https://www.wikipedia.org/` (Public Domain)
Штампа и повез: ТРИ О д.о.о.
Тираж: 300 примерака

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

510.6(075.8)

ИКОДИНОВИЋ, Небојша, 1973-
Увод у математичку логику / Небојша Икодиновић. - 1. изд. - Београд : Универзитет, Математички факултет, 2023 ([Аранђеловац] : Три О). - 188 стр. : илустр. ; 26 cm

Тираж 300. - Напомене уз текст. - Библиографија: стр. 177-178. - Регистар.

ISBN 978-86-7589-177-2

а) Математичка логика

COBISS.SR-ID 124539913

© Математички факултет, 2023
Сва права су задржана. Ниједан део ове публикације не може бити репродукован нити смештен у систем за претраживање и трансмитовање у било ком облику, електронски, механички, фотокопирањем, снимањем или на други начин, без претходне писмене дозволе идавача.

Садржај

Предговор 5

0. Исказна алгебра 7

0.1 Исказне формуле (одн. логички изрази) 8
0.2 Еквивалентне трансформације 17

1. Математичка индукција 25

1.1 Природни бројеви и принцип математичке индукције 26
1.2 Формалне граматике и формалне теорије 35
1.3 Исказни рачун Ł (Формална теорија Ł) 48

2. Природна дедукција 59

2.1 Исказна природна дедукција 60
2.2 Чист предикатски језик 68
2.3 Предикатска природна дедукција 76

3. Теорија **ZF** 85

3.1 Аксиоме изградње скупова 86
3.2 Основни концепти савремене математике 92
3.3 **ZF** теорија 116

4. Заснивање математике 127

4.1 Кардиналност скупа 128
4.2 Аксиома избора 135
4.3 Структуре првог реда 146
4.4 Квантификатор $\mathcal{U}$-скоро свуда 163

Литература (и предлози за читање) 177

Индекс 179

Белешке 182

П

К
ња
мате
руко
коме
ни д
су (
јем
кона

К

- сн
  чи
  до
  ба
- до

Ре
ју са
кључ
Прв
ма, а
Деде
ди д
иска
осно
То п
су и
дана
логи
теор
орем
Кроз
малн
рачу
мо је
Овај
Жел
је мо
деду
посе
вио
ни ра

Предговор

Књига је резултат вишегодишњег осмишљавања и припремања курса *Увод у математичку логику*, на првој години студија математике. Неколико генерација студената је пратило настајање рукописа и ово је прилика да им захвалим на конструктивним коментарима и подстицајним дискусијама. Питања која смо једни другима постављали и одговори које смо размењивали често су (пре)усмеравали писање ове књиге. Посебну захвалност дугујем и рецензентима који су примедбама и предлозима утицали на коначан изглед књиге.

Концепт књиге је одређен тежњом да се истакну две ствари:

- снага математичког приступа у проучавању мишљења и закључивања (логика се од античких времена није значајно мењала, док половином 19. века, математика није почела да се њоме бави);
- доприноси које математика може добити од своје логике.[1]

Редослед излагања у овој књизи мање-више одговара развоју савремене математичке логике. Први део књиге одређују два кључна догађаја која су довела до настанка математичке логике. Први догађај је *алгебраизација логике*, започета Буловим радовима, а други догађај је *аритметизација логике*, започета радовима Дедекинда, Фрегеа и других, и која у Геделовим радовима доводи до спектакуларних резултата. Зато књига почиње поглављем о исказној алгебри и њеним законитостима. У следећем поглављу, основу свих разматрања чини *принцип математичке индукције*. То поглавље је посвећено формалним језицима и теоријама, који су изворно развијани по узору на аритметику. *Формални рачуни* данас заузимају веома значајно место у применама математичке логике, а посебно у развоју рачунарства. Сходно томе, формалне теорије су сликовито представљење као *машине за доказивање теорема*, чиме су истакнути рачунски аспекти вештине доказивања. Кроз примере и задатке уведен је велики број значајних формалних система: поред исказног рачуна, наведени су и формални рачуни група, уређења, мрежа, итд. Следеће поглавље издваја само један рачун – Природну дедукцију за чист предикатски језик. Овај рачун најбоље представљају речи његовог творца, Генцена: *Желео сам да конструишем формализам који ће бити близак, што је могуће више, стварном закључивању.* Заиста, правила природне дедукције веома лепо истичу употребу сваког логичког симбола, посебно квантификатора.[2] Теорија скупова, чије је темеље поставио Кантор, заузима централно место у књизи: уведен је *формални рачун* **ZF** за рад са скуповима; а затим је разрађен стандардни

[1] Амерички математичар М. Дејвис (1928–2023) је своју књигу *На логички погон* посветио једном великом доприносу математичке логике – открићу рачунара. У уводу те књиге аутор примећује: *Рачунар је заправо логичка машина. Он је настао на основу прочишћених увида које је значајни број логичара развијао . . .*

[2] Подсећамо на чувени Витгенштајнов (1889–1951) слоган: *Не питај за значење речи, питај за њену употребу у језику.*

„речник” савремене математике. Рачун **ZF**, и његово проширење аксиомом избора **ZFC**, представљају оквир да се прецизира семантика (значење) разноврсних формалних система, а посебно за предикатске језике. Сходно томе, у последњем поглављу се уводи појам структуре и разматра се концепт последице, одн. њени синтаксни и семантички аспекти. Књига се завршава фундаметалним резултатима[3] на којима почивају веома важне примене савремене математичке логике у разним областима математике.

[3] теорема о ултрафилтеру, теорема компактности, Ремзијева теорема итд.

Садржај је подељен у пет поглавља.

0. Исказна алгебра: Поднаслов овог поглавља би могао бити *алгебарски идентитети и еквивалентне трансформације*, јер је исказна алгебра изложена аналогно познатим бројевним алгебрама.

1. Математичка индукција: Централно место поглавља заузима 'пар екселанс резоновање' (према речима славног математичара Поенкареа) засновано на принципу математичке индукције. Принцип математичке индукције је изложен у контексту природних бројева, а затим је проширен на формалне граматике и формалне теорије. Једна формална теорија је посебно издвојена – *исказни рачун* Ł.

2. Природна дедукција: Систем природне дедукције изложен је најпре за исказну логику, а затим за тзв. чисту предикатску логику. Интерпетација предикатског језика је поменута само узгредно, као подршка интуитивном разумевању језика. Главно место заузимају правила природне дедукције и њихова употреба, која на својеврстан начин одређује и значење симбола.

3. Теорија скупова: Језик и аксиоме теорије скупова су представљење као заједнички оквир разних математичких дисциплина. Централно место поглавља представља листа основних концепата савремене математике.

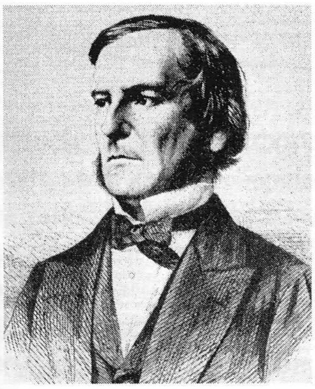
4. Заснивање математике: Последње поглавље обједињује сва претходна и поставља основе за многе области математике. Сасвим уопштено говорећи, поглавље описује главна уопштења идеје *бројања*: (1) поређење скупова по кардиналности; (2) могућност да се скупови добро уреде (и тиме *продужи* принцип индукције); (3) изграђивање бројевних структура (рационалних и реалних бројева).

Београд, јун 2023 Аутор

0. Исказна алгебра

Искористимо симбол 1, тј. јединицу, да означимо универзум ...

Џорџ Бул, прва реченица његовог чланка *Математичка анализа логике* (Mathematical Analysis of Logic), објављеног 1847. године, који се често сматра првим радом савремене математичке логике



Џорџ Бул (1815–1864) је био енглески математичар. Потпуно иновативни приступ логици, Бул је изложио у свом тексту *Математичка анализа логике* (са поднасловом – *есеј о једном рачуну дедуктивног закључивања*), штампаном 1847. године. Булово најважније дело је *Истраживање закона мишљења на којима се заснивају математичке теорије логике и вероватноће*, објављено 1854. године. Сматра се да су Буловим алгебрама постављени темељи савременог, информационог доба.

0.1 **Исказне формуле (одн. логички изрази)**

Увод. Реченице:

1. *Земља се окреће око Сунца или се Земља не окреће око Сунца.*[4]
2. *Број* $1,4142$ *јесте решење једначине* $x^2 = 2$ *или* $1,4142$ *није решење једначине* $x^2 = 2$.

имају исту структуру „··· ***или не*** ···", и управо због тога их сматрамо тачним без обзира на то да ли је исказ који се налази на месту тачкица тачан или нетачан. Одавде се јасно види значај везника *или* и *не* у структури наведених реченица. Још много аналогних примера можемо саставити. Анализирајмо даље и следећа два закључивања.

Ако некоме кажемо	*Ако си ти у праву, онда сам ја луд.*
и додамо	*Ја нисам луд.*
саговорник ће извести закључак	*Ти ниси у праву.*

Знамо да важи	*Ако је четвороугао* $ABCD$ *квадрат, онда је* $ABCD$ *правоугаоник.*
и ако уочимо да	*Четвороугао* $ABCD$ *није правоугаоник.*
закључујемо да	*Четвороугао* $ABCD$ *није квадрат.*

Ова два закључивања, иако се односе на потпуно различите ситуације, суштински се не разликују.

Претпоставке:	*Ако* $\cdots$, *онда* $***$.
	Не $***$.
Закључак:	*Не* $\cdots$.

И овога пута, исправност наведених закључивања оправдавамо везницима „*Ако* $\cdots$, *онда* $***$" и „*Не* $***$" не обазирући се много на смисао реченица које стоје уместо $\cdots$ и $***$.

План

- логичке операције: конјункција, дисјункција, импликација, еквиваленција, негација
- исказне формуле (индуктивна дефиниција): потформуле, дрво формуле
- валуација исказних слова; истинитосна вредност формуле
- задовољиве формуле
- таутологије; списак важних таутологија

Исказна алгебра, ~~ин~~ инд. деф. дрво, потформ., вал. задов. форм., таут., важне таут.

[4] Током људске историје, исказ: *Земља се окреће око Сунца* некада је сматран нетачним, а некада тачним. Без обзира на то, увек се знало да је тачан исказ: *Земља се окреће око Сунца или Земља се не окреће око Сунца.*

Шаблоне закључивања, попут оних из претходног примера, описаћемо посебном врстом алгебарских израза, тзв. логичким изразима. У грађењу тих израза, главну улогу имају следећи *логички везници*, одн. *логичке операције*: *и*, *или*, *не*, *ако . . . онда . . .* , *ако и само ако*. Помоћу њих градимо сложене изразе полазећи од неких једноставних. Вредност сложенијих израза одређујемо само на основу вредности једноставнијих израза и таблица придружених логичким везницима (операцијама). Ово начело, које је у основи дефиниције везника, познато је као **принцип истинитосне функционалности**. За сваки везник, истинитосном таблицом је одређена одговарајућа (рачунска) операција са *истином* и *лажи*, које редом означавамо 1 и 0.

$\neg$	
0	1
1	0

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\Rightarrow$	0	1
0	1	1
1	0	1

$\Leftrightarrow$	0	1
0	1	0
1	0	1

Ове таблице одређују основне **логичке операције**:
- негација $\neg$ – *не* (унарни везник),
- конјункција[5] $\wedge$ – *и* (бинарни везник),
- дисјункција $\vee$ – *или* (бинарни везник),
- импликација $\Rightarrow$ – *ако . . . , онда . . .* (бинарни везник),
- еквиваленција $\Leftrightarrow$ – *ако и само ако*[6] (бинарни везник).

Скуп истинитосних вредности $\{0, 1\}$, заједно са логичким операцијама представља тзв. **исказну алгебру**:

$$(\{0,1\}, \vee, \wedge, \neg, \Rightarrow, \Leftrightarrow, 0, 1)$$

Попут бројевних израза које користимо бавећи се неком бројевном алгебром (коју чини скуп бројева са одговарајућим операцијама), градимо и алгебарске изразе прилагођене исказној алгебри. Ове алгебарске изразе називамо **исказним формулама**. Променљиве су најједноставније исказне формуле; сложеније исказне формуле добијамо применом логичких операција на изграђене формуле.

Пример 1. Исказне формуле, тј. изразе исказне алгебре, можемо замишљати као алгебарски опис структуре исказа – реченице чији нам смисао није важан већ само то да ли су тачне или нетачне. Ако променљиве p, q, r означавају неке једноставне исказе, онда формула:
- $(p \wedge q) \Rightarrow r$ представља сложени исказ „*ако p и q, онда r*”;
- $p \vee \neg p$ представља сложени исказ „*p или не p*”; итд.

Када су познате истинитосне вредности исказа p, q, r, применом таблица за везнике рачунамо истинитост наведених исказа. На пример, ако је $p = 1$, $q = 0$, $r = 0$, онда је истинитосна вредност исказа $(p \wedge q) \Rightarrow r$ једнака $(1 \wedge 0) \Rightarrow 0 = 0 \Rightarrow 0 = 1$.

Исказне формуле дефинишемо као и било коју другу врсту израза – *индуктивном дефиницијом*.

[5] Према савременом правопису, реч *конјункција* се не пише са њ него са нј, као *конјунктив*, *инјекција* и сл.

[6] Уместо *ако и само ако*, често се краће пише *акко*. Слично је и у другим језицима; нпр. на енглеском језику, скраћеница за if and only if је iff.

Приликом превођења формула на говорни језик, и обрнуто, треба узети у обзир и језичке синониме који се користе за импликацију. Исказ облика *Ако p онда q*, можемо формулисати и на један од следећих начина:
- из p следи q,
- p имплицира q,
- p је довољан услов за q,
- q је потребан услов за p.

Најпре прецизирамо које симболе користимо при грађењу исказних формула. Исказне формуле градимо од:

- исказних слова (или исказних променљивих) $a, b, c, \ldots, p, q, r, \ldots, p_1, q_1, \ldots$, претпостављајући да их има неограничено много,
- логичких константи $\top$ и $\bot$,
- логичких везника $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$,

употребљавајући заграде на уобичајени начин.

Логичку константу $\top$ замишљамо као ознаку неког исказа који је тачан, а $\bot$ као ознаку исказа који је нетачан.

Дефиниција 1. [**Индуктивна дефиниција исказних формула**] *Исказне формуле градимо применом следећих правила:*

- *Исказна слова и логичке константе су исказне формуле. Називамо их и атомским исказним формулама.*
- *Ако је α исказна формула, онда је и $\neg\alpha$ исказна формула;*
- *ако су α и β исказне формуле, онда су и $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \Rightarrow \beta)$, $(\alpha \Leftrightarrow \beta)$ исказне формуле.*

Наведеном (индуктивном) дефиницијом најпре су уведене најједноставније исказне формуле: свако исказно слово и свака логичка константа представља једну исказну формулу. Затим је прецизирано како се формирају сложеније исказне формуле: полазећи од најједноставнијих исказних формула, помоћу наведених правила градимо нове формуле, које даље користимо за изградњу још сложенијих формула. Подразумева се да се исказне формуле могу градити само на овај начин.

Индуктивним дефиницијама се одређују математички објекти саграђени постепено, полазећи од најједноставнијих (основних, базних) објеката; сложенији објекти се граде неким утврђеним правилима примењљивим на већ саграђене, једноставније објекте. На такав начин уводимо све познате врсте алгебарских израза. На пример, мономе градимо од променљивих, симбола за бројеве (константе) и примењујући само операцију множења:

- променљиве и константе су мономи;
- ако су α и β мономи, онда је и $(\alpha \cdot \beta)$ моном.

За целе алгебарске изразе користимо и сабирање и множење:

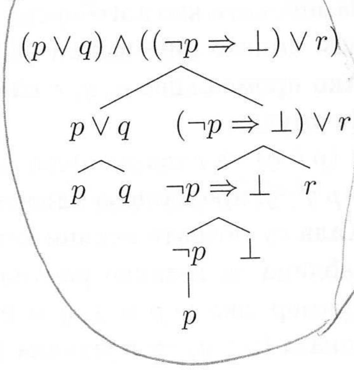
- променљиве и константе су цели алгебарски изрази;
- ако су α и β цели алгебарски изрази, онда су и $(\alpha \cdot \beta)$ и $(\alpha + \beta)$ цели алгебарски изрази моном.

За рационалне изразе дозвољавамо и дељење. За ирационалне и кореновање, итд.

Претпостављамо да су познате уобичајене конвенције о брисању заграда, па их овде нећемо све наводити. Истичемо само договор о приоритету логичких везника: $\neg$ је везник највећег приоритета, за њим следе $\vee$ и $\wedge$ који су подједнаког приоритета, а за њима $\Rightarrow$ и $\Leftrightarrow$, такође једнаког приоритета. Наравно, да бисмо поједноставили запис, изостављамо заграде када год то не доводи до забуне.

Пример 2. Дрво формуле сликовито приказује кораке поступне изградње формуле.

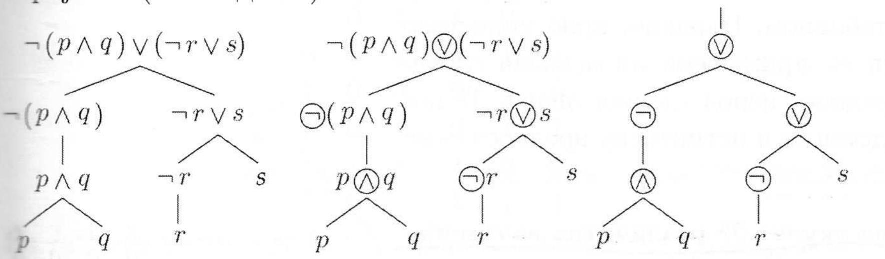
Формула $(p \vee q) \wedge ((\neg p \Rightarrow \bot) \vee r)$ је добијена од формула $p \vee q$ и $(\neg p \Rightarrow \bot) \vee r$, повезаних операцијом $\wedge$. Даље, свака од ових, тзв. потформула је настала од две једноставније формуле повезане операцијом $\vee$: $p \vee q$ од потформула p и q, а $(\neg p \Rightarrow \bot) \vee r$ од $\neg p \Rightarrow \bot$ и r. Сложена потформула $\neg p \Rightarrow \bot$ је добијена повезивањем $\neg p$ и $\bot$ операцијом $\Rightarrow$. Најзад, $\neg p$ је добијена постављањем унарне операције $\neg$ испред слова p. Изградња дрвета се завршава када стигнемо до најједноставнијих потформула, исказних слова и логичких константи. Одговарајуће дрво формуле је приказано десно.



Потформуле неке формуле су њени делови који су и сами формуле, при чему се сматра да је и свака формула потформула саме себе. Потформуле неке исказне формуле јесу формуле које се појављују индуктивном (поступном) изградњом те исказне формуле. Као што је илустровано у претходном примеру, потформуле неке исказне формуле су природно уређене у структуру која подсећа на дрво. Места дрвета где стоје потформуле зову се *чворови*. Сваки чвор има нула или једног непосредног претходника, а непосредних наследника може да има нула, један, или два. Када чвор нема претходника зове се *корен*, а када нема наследника зове се *лист*. Дрво има само један корен. У корену дрвета исказне формуле налази се сама формула, док су листови атомске формуле које учествују у грађењу корена. Чвор дрвета који није лист назива се *унутрашњи чвор*. Сваки унутрашњи чвор дрвета формуле одређен је заправо једним логичким везником. Приказ дрвета формуле се често поједностављује тако што се сваки унутрашњи чвор означава само одговарајућим везником. *Главни везник* формуле јесте логички везник који је последњи уведен приликом њеног грађења, одн. везник који одговара корену поједностављеног приказа дрвета.[10]

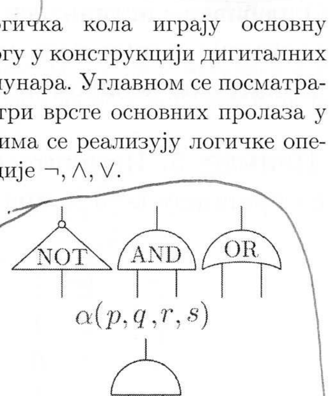
[10] Главни везник неке формуле могли бисмо звати и главна операција (логичког) израза. Главна операција израза истиче се приликом именовања израза. На пример, израз $(a+b)\cdot(a-b)$ називамо *производом*, јер је $\cdot$ главна операција. Слично томе, формулу $p \vee q \Rightarrow p \wedge q$ називамо *импликацијом*, јер је $\Rightarrow$ главни везник. Формула $p \vee (q \Rightarrow p \wedge q)$ је дисјункција, а $(p \vee q \Rightarrow p) \wedge q$ конјункција.

Пример 3. На сликама испод, приказано је дрво исказне формуле $\neg(p \wedge q) \wedge (\neg r \vee s)$ (слика лево) и његова поједностављена варијанта (слика десно).

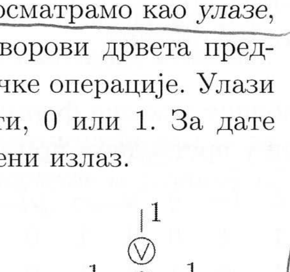


Поједностављену верзију дрвета формуле можемо посматрамо и као тзв. **логичко коло**. Листове дрвета посматрамо као *улазе*, а корен као *излаз* логичког кола. Остали чворови дрвета представљају *пролазе* у којима се реализују логичке операције. Улази и излази могу имати једну од две вредности, 0 или 1. За дате вредности улаза, логичко коло даје јединствени излаз.

Логичка кола играју основну улогу у конструкцији дигиталних рачунара. Углавном се посматрају три врсте основних пролаза у којима се реализују логичке операције ¬, ∧, ∨.



Вредности исказних слова p, q, r, s одређују улазе, и зато полазну формулу означавамо $\alpha(p,q,r,s)$ да бисмо истакли да њена истинитосна вредност зависи од истинитосних вредности слова p, q, r, s. Нпр. ако је $p=1$, $q=0$, $r=0$, $s=1$, онда је:



$$\alpha(1,0,0,1) = \neg(1 \wedge 0) \wedge (\neg 0 \wedge 1) = \cdots = 1$$

Свака исказна формула одређује (логичку) функцију која исти-

нитосним вредностима исказних слова (улаза, аргумената) додељује тачно једну истинитосну вредност посматране формуле.

Формулу α означавамо $\alpha(p_1, p_2, \ldots, p_n)$ када желимо да истакнемо чињеницу да у грађењу формуле α учествују слова p_1, p_2, …, p_n. Додељујући словима $p_1, \ldots, p_n$ редом истинитосне вредности $v_1, \ldots, v_n$ из $\{0, 1\}$, добијамо јединствену *истинитосну* вредност $\alpha(v_1, \ldots, v_n)$. Додељивање истинитосних вредности (0 или 1) исказним словима назива се **валуација** исказних слова. Подразумева се да је истинитосна вредност формуле $\bot$ једнака 0, а истинитосна вредност формуле $\top$ једнака 1.

Уопште, ако је алгебарски израз састављен од променљивих, константи и операција које се појављују у некој конкретној алгебарској структури, онда се вредност тог израза може израчунати када се променљивама доделе конкретне вредности. Посебно, то важи и за исказне формуле, тј. алгебарске изразе који одговарају исказној алгебри.

Пример 4. Истинитосну вредност формуле $(p \Rightarrow q) \wedge (q \Rightarrow p)$, за $p = 1$, $q = 0$, рачунамо користећи следећи сажети запис:

$(p$	$\Rightarrow$	$q)$	$\wedge$	$(q$	$\Rightarrow$	$p)$
1		0		0		1
	0				1	
			0			

или једноставније

$(p$	$\Rightarrow$	$q)$	$\wedge$	$(q$	$\Rightarrow$	$p)$
1	0	0	**0**	0	1	1

Најпре испод исказних слова записујемо истинитосне вредности одређене валуацијом, а затим испод логичких везника вредности одређене одговарајућом таблицом. Наравно, прво уписујемо вредности испод везника који су примењени на исказна слова, да бисмо на крају уписали вредност испод главног знака. Та последња уписана вредност представља и истинтосну вредност саме формуле.

За n исказних слова, постоји укупно 2^n различитих валуација. Одређивање истинитосних вредности неке формуле за све могуће валуације њених исказних слова приказујемо у облику таблице познате под називом *истинитосна таблица*.

p	q
0	0
0	1
1	0
1	1

p	q	r
0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

p	q	r	s
0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
1	1	0	1
1	1	1	0
1	1	1	1

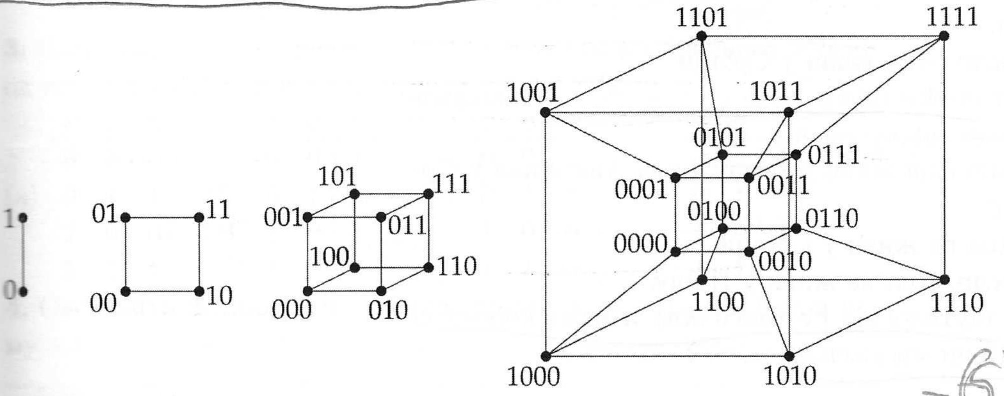
Пример 5. Истинитосну таблицу исказне формуле формирамо по принципу који је примењен у претходном примеру.

$(p$	$\Rightarrow$	$q)$	$\wedge$	$(\neg$	q	$\vee$	$\neg$	$p)$
0	1	0	**1**	1	0	1	1	0
0	1	1	**1**	0	1	1	1	0
1	0	0	**0**	1	0	1	0	1
1	1	1	**0**	0	1	0	0	1

Из практичних разлога, све валуације за n исказних слова набрајамо на следећи систематичан начин: Испод сваког појављивања првог слова наводимо 2^{n-1} пута вредност 0, па 2^{n-1} пута вредност 1; затим испод сваког појављивања другог слова прво наводимо

2^{n-2} пута 0, па затим 2^{n-2} пута 1, па 2^{n-2} пута поново 0, и најзад у још 2^{n-2} пута 1, и тако даље, до n-тог слова испод кога наизменично уписујемо 0 и 1.

Скуп свих валуација n исказних слова назива се и n-димензионални Булов простор и представља се n-димензионалном коцком.



Дефиниција 2. *Формула α је* **задовољива** *ако постоји валуација исказних слова за коју је вредност формуле α једнака* 1.

Пример 6. Формула $p \wedge \neg(q \Rightarrow r)$ је задовољива.

p	$\wedge$	$\neg$	$(q$	$\Rightarrow$	$r)$
0	**0**	0	0	1	0
0	**0**	0	0	1	1
0	**0**	1	1	0	0
0	**0**	0	1	1	1
1	**0**	0	0	1	0
1	**0**	0	0	1	1
1	**1**	1	1	0	0
1	**0**	0	1	1	1

Из таблице видимо да је дата формула тачна за валуацију $p = 1$, $q = 1$, $r = 0$.

Проблем испитивања задовољивости исказних формула краће се назива САТ-проблем (енг. satisfiability – задовољивост). Препоручујемо читаоцу да се путем интернета детаљније информише о овом проблему и његовом значају у савременој математици.

У уводном примеру (стр. 8) најављен је значај исказних формула чија истинитосна вредност не зависи од валуације исказних слова.

Формула $p \vee \neg p$ је истинита и у случају да је $p = 0$, као и да је $p = 1$.

Дефиниција 3. *Исказна формула α је* **таутологија** *ако је за сваку валуацију исказних слова вредност формуле α једнака* 1. *Да је α таутологија означавамо $\models \alpha$.*

Пример 7. Формуле $p \wedge (p \Rightarrow q) \Rightarrow q$ и $(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$ су таутологије (а самим тим и задовољиве):

p	$\wedge$	$(p$	$\Rightarrow$	$q)$	$\Rightarrow$	q
0	0	0	1	0	**1**	0
0	0	0	1	1	**1**	1
1	0	1	0	0	**1**	0
1	1	1	1	1	**1**	1

$(p$	$\Rightarrow$	$q)$	$\wedge$	$\neg$	q	$\Rightarrow$	$\neg$	p
0	1	0	1	1	0	**1**	1	0
0	1	1	0	0	1	**1**	1	0
1	0	0	0	1	0	**1**	0	1
1	1	1	0	0	1	**1**	0	1

О значају таутологија, пре свега при описивању закона мишљења, биће речи касније. За сада, истичемо само да се таутологија $p \wedge (p \Rightarrow q) \Rightarrow q$ (тзв. modus ponens) препознаје у следећем свакодневном закључивању:

$\dfrac{p \quad p \Rightarrow q}{q}$ (MP)

1. Аца живи у Нишу.
2. Ако Аца живи у Нишу, онда Аца живи у Србији.

Дакле, Аца живи у Србији.

Такође, и таутологију modus tolens $(p \Rightarrow q) \wedge \neg q \Rightarrow \neg p$ свакодневно користимо приликом закључивања:

$\dfrac{p \Rightarrow q \quad \neg q}{\neg p}$ (MT)

1. Ако Аца живи у Нишу, онда Аца живи у Србији.
2. Аца не живи у Србији.

Дакле, Аца не живи у Нишу.

Слободно говорећи, таутологије су (логички) изрази којима се описују основни шаблони мишљења.

Одељак завршавамо списком неких важних таутологија (читаоцима препуштамо проверу да су ове формуле заиста таутологије). Наведене формуле се лакше памте ако 0 и 1 схватимо као бројеве и логичке операције опишемо на следећи начин: за $x, y \in \{0,1\}$, $x \vee y = \max\{x, y\}$, $x \wedge y = \min\{x, y\}$, (при чему се ослањамо на уобичајени поредак $0 < 1$), $\neg x = 1 - x$ („$-$" је знак за одузимање). Такође, ваља приметити да импликација $x \Rightarrow y$ има вредност 1 ако и само ако је $x \leqslant y$.

Списак важних таутологија:

Својства импликације:

$\models p \Rightarrow p$

$\models \bot \Rightarrow p$ $\quad \models p \Rightarrow \top$

$\models (p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)$ *транзитивност импликације*

$\models (p \Rightarrow q) \vee (q \Rightarrow p)$ *линеарност импликације*

Својства конјункције:

$\models p \wedge q \Rightarrow p$ $\quad \models p \wedge q \Rightarrow q$

$\models (r \Rightarrow p) \wedge (r \Rightarrow q) \Rightarrow (r \Rightarrow p \wedge q)$ *формула $p \wedge q$ је највеће доње ограничење за p и q*

Својства дисјункције:

$\models p \Rightarrow p \vee q$ $\quad \models q \Rightarrow p \vee q$

$\models (p \Rightarrow r) \wedge (q \Rightarrow r) \Rightarrow (p \vee q \Rightarrow r)$ *формула $p \vee q$ је најмање горње ограничење за p и q*

Својства негације:

$\models \bot \Rightarrow q$ ex falso quodlibet – *из лажне претпоставке следи све*

$\models (p \Rightarrow q) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \neg p)$ reductio ad absurdum – *свођење на противречност*

$\models (p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p)$ *закон контрапозиције*

$\models p \Leftrightarrow \neg\neg p$ *закон двојне негације*

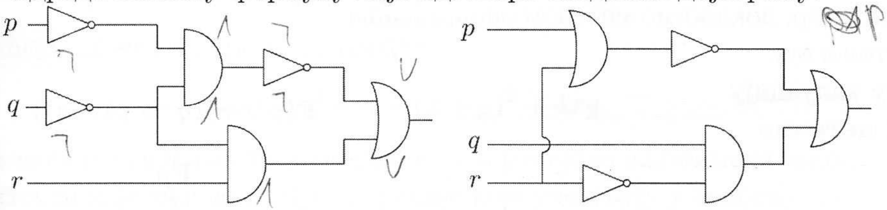
$\models p \vee \neg p$ *закон искључења трећег*

▼ Задаци и додаци

1. Нацртати дрво формуле:
(а) $p \wedge \neg(q \Rightarrow r)$ (б) $p \wedge \neg q \Rightarrow r$ (в) $(p \wedge \neg q) \Rightarrow r)$

битно

2. Одреди исказну формулу која одговара следећем дијаграму:



3. Наћи бар једну формулу α чија истинитосна вредност зависи од исказних слова p и q као што је дато у табели.

	p	q	α		p	q	α		p	q	α		p	q	α
(а)	0	0	0	(б)	0	0	1	(в)	0	0	0	(г)	0	0	1
	0	1	1		0	1	0		0	1	1		0	1	1
	1	0	0		1	0	1		1	0	0		1	0	1
	1	1	1		1	1	1		1	1	0		1	1	0

4. Саставити истинитосне таблице формула $p_1 * (p_2 * p_1)$, при чему $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow, \Leftarrow\}$.

Додатак

Приликом испитивања задовољивости неке формуле, трагање за валуацијама се може спровести анализом структуре задате формуле, користећи следеће чињенице које директно произлазе из истинитосних таблица:

($\neg T$) Ако је $\neg\alpha$ **тачно**, онда је α **нетачно**;
($\neg N$) Ако је $\neg\alpha$ **нетачно**, онда је α **тачно**;
($\wedge T$) Ако је $\alpha \wedge \beta$ **тачно**, онда је α **тачно** и β је **тачно**;
($\wedge N$) Ако је $\alpha \wedge \beta$ **нетачно**, онда је α **нетачно** или је β **нетачно**;
($\vee T$) Ако је $\alpha \vee \beta$ **тачно**, онда је α **тачно** или је β **тачно**;
($\vee T$) Ако је $\alpha \vee \beta$ **нетачно**, онда је α **нетачно** и β је **нетачно**;
($\Rightarrow T$) Ако је $\alpha \Rightarrow \beta$ **тачно**, онда је α **нетачно** или је β **тачно**;
($\Rightarrow N$) Ако је $\alpha \Rightarrow \beta$ **нетачно**, онда је α **тачно** и β је **нетачно**.

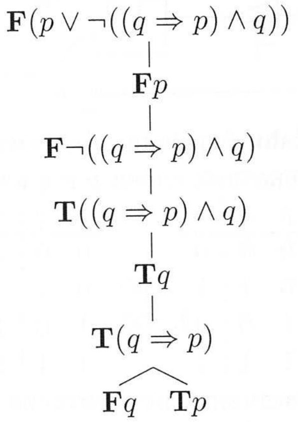
Ако изјаве '*формула φ је тачна*' и '*формула φ је нетачна*' редом краће означимо $\mathbf{T}\varphi$ и $\mathbf{F}\varphi$, горња правила можемо сликовитије приказати на следећи начин:

$\mathbf{T}\neg\alpha$	$\mathbf{F}\neg\alpha$	$\mathbf{T}\alpha\wedge\beta$	$\mathbf{F}\alpha\wedge\beta$	$\mathbf{T}\alpha\vee\beta$	$\mathbf{F}\alpha\vee\beta$	$\mathbf{T}\alpha\Rightarrow\beta$	$\mathbf{F}\alpha\Rightarrow\beta$
$\mathbf{F}\alpha$	$\mathbf{T}\alpha$	$\mathbf{T}\alpha$	$\mathbf{F}\alpha$ $\quad$ $\mathbf{F}\beta$	$\mathbf{T}\alpha$ $\quad$ $\mathbf{T}\beta$	$\mathbf{F}\alpha$	$\mathbf{F}\alpha$ $\quad$ $\mathbf{T}\beta$	$\mathbf{T}\alpha$
		$\mathbf{T}\beta$			$\mathbf{F}\beta$		$\mathbf{F}\beta$

Полазећи од чвора $\mathbf{F}\varphi$ (тј. претпоставке да је φ нетачно), и примењујући наведена правила док год је могуће, добијамо тзв. *истинитосно дрво* или *табло*. Путања од корена до листа је *затворена* уколико садржи формулу и њену негацију; у супротном, путања је *отворена*. Ако конструишемо табло са кореном $\mathbf{F}\varphi$, који садржи неку отворену грану, закључујемо да постоји валуација за коју је формула φ нетачна (валуацију читамо са те отворене гране). У супротном, ако су затворене све гране таблоа са кореном $\mathbf{F}\varphi$, закључујемо да не постоји валуација за коју је формула нетачна, одн. да је φ таутологија.

Описани метод доказивања да је формула таутологија познат је и као метод оповргавања. На пример, докажимо методом оповргавања да је $p \vee \neg((q \Rightarrow p) \wedge q)$ таутологија.

Претпоставимо да је за неку валуацију формула $p \vee \neg((q \Rightarrow p) \wedge q)$ **нетачна**.
Тада је p **нетачно** и
$\neg((q \Rightarrow p) \wedge q)$ **нетачно**,
односно $(q \Rightarrow p) \wedge q$ је **тачно**.
Из последње чињенице следи да је
q **тачно** и
да је $q \Rightarrow p$ **тачно**.
Како је $q \Rightarrow p$ тачно, онда
q мора бити **нетачно** или
p мора бити **тачно**,
што је немогуће, јер смо већ закључили да је p **нетачно** и q **тачно**.



5. Наћи, уколико постоји, бар једну валуацију исказних слова тако да формула $(p \Rightarrow q) \wedge (p_1 \Rightarrow q_1) \Rightarrow ((p \Rightarrow p_1) \Rightarrow (q \Rightarrow q_1))$ добије вредност 1 и бар једну валуацију исказних слова тако да формула добије вредност 0.

6. Доказати да су следеће формуле таутологије:
(а) $p \vee \neg((q \Rightarrow p) \wedge q)$
(б) $((p_1 \Rightarrow p_2) \Rightarrow p_3) \Rightarrow ((p_3 \Rightarrow p_1) \Rightarrow (p_4 \Rightarrow p_1))$
(в) $((((p \Rightarrow q) \Rightarrow (\neg r \Rightarrow \neg s)) \Rightarrow r) \Rightarrow t) \Rightarrow ((t \Rightarrow p) \Rightarrow (s \Rightarrow p))$

7. Испитати да ли су следеће формуле таутологије. У случају да формула није таутологија, наћи валуацију за коју је нетачна.
(а) $(p \Rightarrow \neg p) \Leftrightarrow \neg p$
(б) $p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$
(в) $((p \Rightarrow q) \Rightarrow q) \Rightarrow p$
(г) $p \Rightarrow ((q \Rightarrow r) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r)))$
(д) $(p \wedge q \Rightarrow r) \Rightarrow ((p \vee r \Rightarrow p) \Rightarrow (q \Rightarrow p))$
(ђ) $((p \vee q) \wedge (p \Rightarrow r) \wedge (q \Rightarrow s) \wedge \neg(r \vee s)) \Rightarrow ((r \Rightarrow p) \wedge (s \Rightarrow q))$
(е) $(p \Rightarrow (\neg q \vee (r \vee s))) \wedge \neg(p \Rightarrow s) \Rightarrow \neg q$
(ж) $(p \Rightarrow (q \Rightarrow r)) \wedge (p \wedge r \Rightarrow \neg s) \Rightarrow (p \wedge s \Rightarrow \neg q)$

8. Доказати да за све формуле $\alpha, \beta, \gamma, \delta$ важи:
(а) ако је $\models \alpha \vee \beta$ и $\models \neg\alpha \vee \gamma$, онда је $\models \beta \vee \gamma$;
(б) ако је $\models \alpha \vee \beta$, $\models \alpha \Rightarrow \gamma$ и $\models \beta \Rightarrow \delta$, онда је $\models \gamma \vee \delta$;
(в) ако је $\models \neg\alpha \vee \beta$ и $\models \neg\beta \vee \neg\gamma$, онда је $\models \alpha \Rightarrow \neg\gamma$.

9. Ако је $\models \alpha \Rightarrow \beta$ и $\models \neg\alpha \Rightarrow \beta$, испитати да ли формула $\neg\beta$ мора бити таутологија?

10. Нека су α и β исказне формуле које немају ниједно заједничко исказно слово. Доказати да су следећи услови еквивалентни:
(а) $\alpha \Rightarrow \beta$ је таутологија;
(б) бар једна од формула $\neg\alpha$ или β је таутологија.

11. Ако су α и β задовољиве формуле, такве да је $\models \alpha \Leftrightarrow \neg\beta$, доказати да постоји бар једно исказно слово које се појављује и у α и у β.

0.2. Еквивалентне трансформације

Увод. Доказ да вредност израза

$$(x-y)^2+4-(x+y)^2+4xy$$

не зависи од вредности промељивих x и y почива на примени законитости које задовољавају операције које учествују у грађењу израза. Познато је да за све бројеве a и b важи једнакост позната као *разлика квадрата* $a^2-b^2=(a-b)(a+b)$. Штавише, та једнакост важи када су A и B било који изрази: $A^2-B^2=(A-B)(A+B)$. Користећи ово својство и друге познате особине, добијамо:

$$\begin{aligned}(x-y)^2+4-(x+y)^2+4xy &= (x-y)^2-(x+y)^2+4xy+4\\ &= (x-y-(x+y))(x-y+(x+y))+4xy+4\\ &= -4xy+4xy+4\\ &= 4\end{aligned}$$

Докажимо да истинтосна вредност следеће формуле не зависи од истинитосних вредности исказних слова која се у њој појављују:

$$p\Rightarrow(q\Rightarrow(s\Rightarrow(t\Rightarrow(u\Rightarrow u)))).$$

Формула садржи пет исказних слова, па би формирање истинитосне таблице захтевало испитивање $2^5=32$ случаја. Уместо тога, једноставније је уочити неке алгебарске законитости које задовољава логичка операција $\Rightarrow$. Довољно је учити следеће две чињенице:

- вредност формуле $a\Rightarrow a$ је 1, без обзира на вредност слова a,
- вредност формуле $a\Rightarrow 1$ је 1, без обзира на вредност слова a.[16]

Дакле,

$$\begin{aligned}p\Rightarrow(q\Rightarrow(s\Rightarrow(t\Rightarrow(u\Rightarrow u)))) &= p\Rightarrow(q\Rightarrow(s\Rightarrow(t\Rightarrow 1)))\\ &= p\Rightarrow(q\Rightarrow(s\Rightarrow 1))\\ &= p\Rightarrow(q\Rightarrow 1)\\ &= p\Rightarrow 1\\ &= 1\end{aligned}$$

Овај низ једнакости потврђује да је вредност дате формуле увек 1 без обзира на вредности слова која се у формули појављују.

План

- супституција; инстанца формуле
- еквивалентне формуле; логички идентитети
- својства еквивалентности; еквивалентне трансформације
- конјунктивна и дијсунктивна нормална форма.

[16] Избегавамо употребу ознаке $\top$, да бисмо јасније истакли суштину примера.

Исказна слова се зову још и *исказне променљиве*. Уопште у математици, променљива је симбол везан за супституцију, тј. замену, без изузетка, свих јављања тог симбола неким истим изразом. Користимо следеће ознаке:

- $[p/\varphi]$ означава истовремену замену слова p формулом φ;
- $\alpha[p/\varphi]$ означава формулу добијену када се у α сва појављивања слова p замене формулом φ.

Резултат супституције се зове супституциона инстанца, или само **инстанца**. У некој исказној формули, уместо променљивих могу да се постављају произвољне исказне формуле, и добијене инстанце су онда опет исказне формуле.

Пример 8. Ако је α формула $\neg(p \Rightarrow q) \Rightarrow p \land \neg q$, онда је:

- $\alpha[p/p \lor r]$ формула $\neg(p \lor r \Rightarrow q) \Rightarrow (p \lor r) \land \neg q$;
- $\alpha[q/r \Rightarrow \neg s]$ формула $\neg(p \Rightarrow (r \Rightarrow \neg s)) \Rightarrow p \land \neg(r \Rightarrow \neg s)$;
- $\alpha[s/p \Rightarrow \neg r]$ формула α, тј. $\neg(p \Rightarrow q) \Rightarrow p \land \neg q$, јер се s не појављује у α.

Приметимо да је формула α, тј. $\neg(p \Rightarrow q) \Rightarrow p \land \neg q$ таутологија. Да ли су формуле $\alpha[p/p \lor r]$, $\alpha[q/r \Rightarrow \neg s \land t]$ и $\alpha[s/p \Rightarrow \neg r]$ такође таутологије?

$\neg$	$(p$	$\Rightarrow$	$q)$	$\Rightarrow$	p	$\land$	$\neg$	q
0	0	1	0	**1**	0	0	1	0
0	0	1	1	**1**	0	0	0	1
1	1	0	0	**1**	1	1	1	0
0	1	1	1	**1**	1	0	0	1

Посебно истичемо једну очигледну чињеницу: *свака инстанца таутологије је такође таутологија.*

Теорема 1. *Ако је α таутологија, онда је и $\alpha[p/\varphi]$ такође таутологија, за било коју формулу φ.*

Доказ ове теореме изостављамо јер сама теорема представља очигледну чињеницу, а строг доказ се спроводи *индукцијом по сложености формуле* о чему ће бити речи у наредном поглављу.

Пример 9. Знамо да су формуле

$$p \land (p \Rightarrow q) \Rightarrow q \text{ и } (p \Rightarrow q) \land \neg q \Rightarrow \neg p$$

таутологије. Применом претходне теореме закључујемо да су и њихове инстанце

$$\varphi \land (\varphi \Rightarrow \psi) \Rightarrow \psi \text{ и } (\varphi \Rightarrow \psi) \land \neg\psi \Rightarrow \neg\varphi,$$

такође таутологије, за било које формуле φ и ψ. Прецизније, до закључка долазимо вишеструком применом претходне теореме. Наиме, наведене инстанце представљају резултат тзв. *истовремене замене* слова p и q редом формулама φ и ψ. Међутим, оваква врста замене се увек може свести на неколико узастопних замена једног слова неком формулом. Без много детаља, наводимо само један пример. Претпоставимо да у формули α треба *истовремено* заменити слова p и q редом формулама φ и ψ; означимо резултат овакве замене са $\alpha[p/\varphi, q/\psi]$. Изаберимо слово, различито од p и q, које се не појављује у формулама α, φ, ψ, нпр. r и означимо φ' формулу $\varphi[q/r]$, онда је $\alpha[p/\varphi, q/\psi]$ истоветна формули $\alpha[p/\varphi'][q/\psi][r/q]$.

Уопште, формуле $\alpha[p/\varphi, q/\psi]$ и $\alpha[p/\varphi][q/\psi]$ нису исте, уколико се q појављује у φ.

Посебно су важне таутологије које су еквиваленције неке две формуле.

Дефиниција 4. *Формуле α и β су* ***еквивалентне****, у ознаци $\alpha \equiv \beta$, ако α и β имају исте истинитосне вредности за сваку валуацију, тј. ако је $\models \alpha \Leftrightarrow \beta$.*

Приметимо да је $\alpha \equiv \beta$ само други запис чињенице $\models \alpha \Leftrightarrow \beta$.

Издвајамо неке основне парове еквивалентних формула који представљају познате *логичке идентитете*.

Теорема 2. *За било које формуле α, β, γ важи:*

$\mathbf{A}^{\vee}$	$\alpha \vee (\beta \vee \gamma) \equiv (\alpha \vee \beta) \vee \gamma$	$\mathbf{A}^{\wedge}$	$\alpha \wedge (\beta \wedge \gamma) \equiv (\alpha \wedge \beta) \wedge \gamma$
$\mathbf{K}^{\vee}$	$\alpha \vee \beta \equiv \beta \vee \alpha$	$\mathbf{K}^{\wedge}$	$\alpha \wedge \beta \equiv \beta \wedge \alpha$
$\mathbf{D}^{\vee}_{\wedge}$	$\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$	$\mathbf{D}^{\wedge}_{\vee}$	$\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$
$\mathbf{C}^{\vee}$	$\alpha \vee \neg\alpha \equiv \top$	$\mathbf{C}^{\wedge}$	$\alpha \wedge \neg\alpha \equiv \bot$
$\mathbf{N}^{\vee}$	$\alpha \vee \bot \equiv \alpha$	$\mathbf{N}^{\wedge}$	$\alpha \wedge \top \equiv \alpha$
	$\alpha \vee \top \equiv \top$		$\alpha \wedge \bot \equiv \bot$
$\mathbf{I}^{\vee}$	$\alpha \vee \alpha \equiv \alpha$	$\mathbf{I}^{\wedge}$	$\alpha \wedge \alpha \equiv \alpha$
$\mathbf{A}^{\vee}_{\wedge}$	$\alpha \vee (\alpha \wedge \beta) \equiv \alpha$	$\mathbf{A}^{\wedge}_{\vee}$	$\alpha \wedge (\alpha \vee \beta) \equiv \alpha$
DM	$\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$	**DM**	$\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$
	$\alpha \equiv \neg\neg\alpha$		
	$\alpha \Rightarrow \beta \equiv \neg\alpha \vee \beta$		$\alpha \Leftrightarrow \beta \equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$

Доказ. Наведене логичке идентитете добијамо применом теореме 1 на одговарајуће таутологије:

$\models p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r$	$\models p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r$	*закони асоцијативности*
$\models p \vee q \Leftrightarrow q \vee p$	$\models p \wedge q \Leftrightarrow q \wedge p$	*закони комутативности*
$\models p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$	*закони дистрибутивности $\vee$ према $\wedge$*	
$\models p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r)$	*закони дистрибутивности $\wedge$ према $\vee$*	
$\models p \vee \neg p \Leftrightarrow \top$	$\models p \wedge \neg p \Leftrightarrow \bot$	
$\models p \vee \bot \Leftrightarrow p$	$\models p \wedge \top \Leftrightarrow p$	
$\models p \vee \top \Leftrightarrow \top$	$\models p \wedge \bot \Leftrightarrow \bot$	
$\models p \vee p \Leftrightarrow p$	$\models p \wedge p \Leftrightarrow p$	*закони идемпотентности*
$\models p \vee (p \wedge q) \Leftrightarrow p$	$\models p \wedge (p \vee q) \Leftrightarrow p$	*закони апсорпције*
$\models \neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$	$\models \neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$	*Де Морганови закони*
$\models p \Leftrightarrow \neg\neg p$	*закон двојне негације*	
$\models p \Rightarrow q \Leftrightarrow \neg p \vee q$	$\models p \Leftrightarrow q \Leftrightarrow (p \Rightarrow q) \wedge (q \Rightarrow p)$	

Доказе да су ове формуле таутологије остављамо за вежбу. □

Де Морганови закони названи су у част Августа де Моргана (1806–1871), британског математичара.

Неке олакшице приликом записивања формула усвајамо на основу асоцијативности и комутативности конјункције и дисјункције. Асоцијативност дисјункције $\mathbf{A}^{\vee}$, одн. конјункције $\mathbf{A}^{\wedge}$, омогућава да се без употребе заграда записују конјункције, одн. дисјункције више од две исказне формуле:

$$\alpha_1 \wedge \alpha_2 \cdots \wedge \alpha_k, \text{ одн. } \alpha_1 \vee \alpha_2 \cdots \vee \alpha_k, \ k \geqslant 3$$

при чему, наравно, остаје могућност да конјункте, одн. дисјункте здружимо заградама, по потреби. Комутативност дисјункције $\mathbf{K}^{\vee}$, одн. конјункције $\mathbf{K}^{\wedge}$, ослобађа нас бриге о редоследу навођења конјунката, одн. дисјунката.

У наредној теореми издвојамо основна својства еквивалентности.

Теорема 3. *Нека су α, β, γ произвољне исказне формуле:*

(R) $\alpha \equiv \alpha$;

(S) *ако је* $\alpha \equiv \beta$, *онда је и* $\beta \equiv \alpha$;

(T) *ако је* $\alpha \equiv \beta$ *и* $\beta \equiv \gamma$, *онда је и* $\alpha \equiv \gamma$;

(K) *ако је* $\alpha \equiv \beta$ *и* $\gamma \equiv \delta$, *онда је и* $\alpha * \gamma \equiv \beta * \delta$, *за било који везник* $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$; *ако је* $\alpha \equiv \beta$, *онда је и* $\neg\alpha \equiv \neg\beta$;

(S) *ако је* $\alpha \equiv \beta$, *онда је* $\gamma[p/\alpha] \equiv \gamma[p/\beta]$, *за било које слово* p.

Идеја доказа. Еквивалентне формуле су оне које имају једнаке вредности за било коју валуацију. Према томе, наведена својства еквивалентности јесу директне последице одговарајућих својстава једнакости. Приметимо да се тврђења могу формулисати и на следећи начин:
(R) $\models \alpha \Leftrightarrow \alpha$;
(S) из $\models \alpha \Leftrightarrow \beta$ следи $\models \beta \Leftrightarrow \alpha$;
(T) из $\models \alpha \Leftrightarrow \beta$ и $\models \beta \Leftrightarrow \gamma$ следи $\models \alpha \Leftrightarrow \gamma$;
(K) из $\models \alpha \Leftrightarrow \beta$ и $\models \gamma \Leftrightarrow \delta$ следи $\models \alpha * \gamma \Leftrightarrow \beta * \delta$;
(S) из $\models \alpha \Leftrightarrow \beta$ следи $\models \gamma[p/\alpha] \Leftrightarrow \gamma[p/\beta]$. □

Тврђење (S), претходне теореме, познато је и као *теорема о замени еквивалената.*[22] Ако је $\alpha \equiv \beta$, и у некој формули се појављује α као потформула, онда се након замене сваког појављивања формуле α формулом β, добија нова формула еквивалентна полазној. Две еквивалентне формуле увек имају исте истинитосне вредности, па је јасно да свако појављивање једне од тих формула, у некој формули, можемо заменити другом, њој еквивалентном формулом.

[22] Замена еквивалената је у основи тзв. еквивалентних трансформација било каквих алгебарских израза. На пример, знамо да је $x^2 - y^2 = (x-y)(x+y)$, тј. да су изрази $x^2 - y^2$ и $(x-y)(x+y)$ еквивалентни (имају исте вредности за све вредности променљивих x и y), а знамо и да ако појављивање израза $x^2 - y^2$, у неком сложеном изразу, заменимо изразом $(x-y)(x+y)$, добијамо израз еквивалентан полазном сложеном изразу.

Уопштено говорећи, трансформације алгебарских израза су засноване на неким полазним идентитетима и основним својствима једнакости. У случају логичких израза (тј. исказних формула), еквивалентне трансформације су одређене идентитетима издвојеним у теореми 2 и својствима еквивалентности наведеним у теореми 3.

Пример 10. Применом наведених еквиваленција доказаћемо да је формула $(p \vee q) \vee (\neg p \wedge \neg q)$ таутологија:

$$\begin{aligned}
(p \vee q) \vee (\neg p \wedge \neg q) &\equiv ((p \vee q) \vee \neg p) \wedge ((p \vee q) \vee \neg q) && [\mathbf{D}^{\vee}_{\wedge}]\\
&\equiv ((q \vee p) \vee \neg p) \wedge (p \vee (q \vee \neg q)) && [\mathbf{K}^{\vee}, \mathbf{A}^{\vee}]\\
&\equiv (q \vee (p \vee \neg p)) \wedge (p \vee \top) && [\mathbf{A}^{\vee}, \mathbf{C}^{\vee}]\\
&\equiv (q \vee \top) \wedge \top && [\mathbf{C}^{\vee}, \alpha \vee \top \equiv \top]\\
&\equiv \top \wedge \top && [\top \wedge \top \equiv \top]\\
&\equiv \top
\end{aligned}$$

Слично се може показати да исказна формула $(p \vee q) \wedge (\neg p \wedge \neg q)$ није задовољива.

$(p \vee q) \wedge (\neg p \wedge \neg q) \equiv \cdots \equiv \bot$

Еквивалентним трансформацијама сваку исказну формулу преводимо у тзв. *нормалне форме.*

Дефиниција 5. *Формула је у дисјунктивној нормалној форми (днф) ако је облика $D_1 \vee D_2 \vee \cdots \vee D_k$, где је сваки дисјункт D_i облика $\lambda_{i_1} \wedge \cdots \wedge \lambda_{i_\ell}$, и λ_{i_j} су исказна слова или негације исказних слова.*

Формула је у конјунктивној нормалној форми (кнф) ако је облика $K_1 \wedge K_2 \wedge \cdots \wedge K_d$, при чему је сваки конјункт K_i облика $\lambda_{i_1} \vee \cdots \vee \lambda_{i_\ell}$, и λ_{i_j} су исказна слова или негације исказних слова.

Исказна слова и негације исказних слова називају се и *литерали.*

Пример 11. Свака исказна формула је еквивалентна некој формули која је у днф, као и некој формули која је у кнф; еквивалентну днф, односно кнф форму једноставно добијамо из истинитосне таблице. На пример, нека формули α одговара таблица приказана десно. Уочавајући за које валуације формула α има вредност 1, једноставно налазимо днф ове формуле:

x_1	x_2	x_3	α
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	0

$$(\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge \neg x_3).$$

Уочавајући за које валуације формула α има вредност 0 налазимо кнф формуле:

$$(x_1 \vee x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee x_3) \wedge (x_1 \vee \neg x_2 \vee \neg x_3) \wedge (\neg x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee \neg x_2 \vee \neg x_3).$$

Иако нормалне форме неке формуле можемо одредити помоћу њене истинитосне таблице, чешће се примењују еквивалентне трансформације. Дисјунктивна (конјунктивна) нормална форма неке формуле одређује се следећим поступком:

1. елиминисати везник $\Leftrightarrow$ користећи еквиваленцију: $\alpha \Leftrightarrow \beta \equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$;

2. елиминисати везник $\Rightarrow$ користећи еквиваленцију: $\alpha \Rightarrow \beta \equiv \neg\alpha \vee \beta$;

3. док год је могуће примењивати Де Органове законе (тј. док год се све негације не 'спусте' до исказних слова и логичких константи), $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$ и $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$;

4. елиминисати вишеструке негације и негације константи користећи логичке еквиваленције: $\neg\neg\alpha \equiv \alpha$, $\neg\bot \equiv \top$ и $\neg\top \equiv \bot$;

5. на формулу добијену у претходном кораку примењивати еквиваленције које произлазе из дистрибутивног $\mathbf{D}^{\wedge}_{\vee}$ (односно $\mathbf{D}^{\vee}_{\wedge}$), асоцијативног и комутативног закона, уз одговарајућу елиминацију константи, док год се не добије израз у днф (односно кнф).

Наравно, редослед корака можемо по потреби модификовати и прилагодити га датој ситуацији. Поред тога, форме добијене претходним поступком можемо додатно појелноставити применом еквиваленција: $\alpha \vee \alpha \equiv \alpha$, $\alpha \wedge \alpha \equiv \alpha$, $\alpha \vee \neg\alpha \equiv \top$, $\alpha \wedge \neg\alpha \equiv \bot$ итд.

Пример 12. Одредимо нормалне форме формуле

$$\neg(p_1 \Rightarrow p_2) \Rightarrow (\neg p_1 \wedge p_3).$$

ДНФ		КНФ	
	$\neg(p_1 \Rightarrow p_2) \Rightarrow (\neg p_1 \wedge p_3)$		$\neg(p_1 \Rightarrow p_2) \Rightarrow (\neg p_1 \wedge p_3)$
$\equiv$	$\neg\neg(\neg p_1 \vee p_2) \vee (\neg p_1 \wedge p_3)$	$\equiv$	$\neg\neg(\neg p_1 \vee p_2) \vee (\neg p_1 \wedge p_3)$
$\equiv$	$\neg p_1 \vee p_2 \vee (\neg p_1 \wedge p_3)$	$\equiv$	$(\neg p_1 \vee p_2) \vee (\neg p_1 \wedge p_3)$
		$\equiv$	$(\neg p_1 \vee p_2 \vee \neg p_1) \wedge (\neg p_1 \vee p_2 \vee p_3)$
		$\equiv$	$(\neg p_1 \vee p_2) \wedge (\neg p_1 \vee p_2 \vee p_3)$

▼ Задаци и додаци

1. Знак '?' заменити формулом тако да добијене формуле буду таутологије.

$p \wedge \bot \Leftrightarrow ?$ $\quad p \wedge \top \Leftrightarrow ?$ $\quad p \vee \bot \Leftrightarrow ?$ $\quad p \vee \top \Leftrightarrow ?$

$(p \Rightarrow \bot) \Leftrightarrow ?$ $\quad (p \Rightarrow \top) \Leftrightarrow ?$ $\quad (\bot \Rightarrow p) \Leftrightarrow ?$ $\quad (\top \Rightarrow p) \Leftrightarrow ?$

$(p \Leftrightarrow \bot) \Leftrightarrow ?$ $\quad (p \Leftrightarrow \top) \Leftrightarrow ?$

2. Уписати знак $\times$ у квадратић испред формуле која је еквивалентна датој формули.

(а) Формула $p \Rightarrow \neg(q \vee r)$ је еквивалентна формули:

☐ $\neg p \vee (q \vee r)$ ☐ $\neg q \wedge \neg r \Rightarrow \neg p$ ☐ $\neg p \vee \neg(\neg q \Rightarrow r)$

(б) Формула $p \vee \neg q \Rightarrow \neg r$ је еквивалентна формули:

☐ $\neg(p \Rightarrow q) \vee \neg r$ ☐ $\neg(q \Rightarrow p) \vee \neg r$ ☐ $r \Rightarrow \neg p \vee q$

(в) Формула $p \Rightarrow (q \Rightarrow r)$ је еквивалентна формули:

☐ $p \wedge q \Rightarrow r$ ☐ $p \vee q \Rightarrow r$ ☐ $(\neg p \vee \neg q) \vee r$

(г) Формула $p \wedge q \Rightarrow p \vee r$ је еквивалентна формули:

☐ $q \Rightarrow r$ ☐ $r \Rightarrow q$ ☐ $p \vee q \Rightarrow p \wedge r$

3. Да ли су еквивалентне формуле:

(а) $\alpha \Rightarrow (\beta \Rightarrow \gamma)$ и $\beta \Rightarrow (\alpha \Rightarrow \gamma)$;

(б) $\alpha \Rightarrow (\beta \Rightarrow \gamma)$ и $\alpha \Rightarrow (\gamma \Rightarrow \beta)$;

(в) $\alpha \Rightarrow (\beta \Rightarrow \gamma)$ и $\gamma \Rightarrow (\beta \Rightarrow \alpha)$;

(г) $\alpha \Rightarrow (\beta \Rightarrow \gamma)$ и $(\alpha \Rightarrow \beta) \Rightarrow \gamma$?

4. Доказати следеће идентитете:

(а) $(p \wedge q) \vee (r \wedge s) \equiv (p \vee r) \wedge (q \vee r) \wedge (p \vee s) \wedge (q \vee s)$

(б) $(p \vee q) \wedge (r \vee s) \equiv (p \wedge r) \vee (q \wedge r) \vee (p \wedge s) \vee (q \wedge s)$

(в) $p \vee (\neg p \wedge q) \equiv p \vee q$

(г) $p \wedge (\neg p \vee q) \equiv p \wedge q$

(д)[26] $(p \wedge q) \vee (q \wedge r) \vee (r \wedge p) \equiv (p \vee q) \wedge (q \vee r) \wedge (r \vee p)$

(ђ) $\neg(p \vee q) \vee \neg(\neg p \vee q) \equiv \neg q$

(е) $\neg(p \wedge q) \wedge \neg(\neg p \wedge q) \equiv \neg q$

(ж) $(p \wedge q) \vee (\neg p \wedge \neg q) \equiv (p \vee \neg q) \wedge (\neg p \vee q)$

[26] Дедекиндов идентитет. Рихард Дедекинд (1831–1916), немачки математичар

5. Упростити исказну формулу (наћи формулу најмање сложености која је еквивалентна датој формули):
(а) $(p \land \neg q \land \neg r) \lor (p \land q \land \neg r) \lor (p \land q \land r) \lor (p \land \neg q \land r)$
(б) $p \lor (p \land q) \lor (q \land r) \lor (\neg p \land r)$
(в) $(((p \lor q) \land ((\neg p \land \neg q) \lor r)) \lor \neg r) \land q$
6. Ако су формуле $\alpha[p/\top]$ и $\alpha[p/\bot]$ таутологије, да ли α мора бити таутологија? Одговор детаљно образложити.

Додатак
Тврђење претходног задатка се може искористити да се покаже да је нека формула таутологија. Метод је познат под називом *дискусија по исказном слову*: супституцијом константи $\top$ и $\bot$ уместо погодно изабраног исказног слова, добијамо две формуле са мање променљивих за које испитујемо да ли су таутологије.

---

7. Одредити све, до на еквиваленцију, исказне формуле $\alpha(p, q)$ (које садрже само слова p и q) тако да је:
(а) $\models p \land \alpha \Leftrightarrow p \land q$.
(б) $\models (\alpha \land q \Rightarrow \neg p) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \alpha)$
(в) $\models (\alpha \land q \Rightarrow \neg p) \Rightarrow ((p \Rightarrow \neg q) \Rightarrow \alpha)$
8. Одредити, до на еквиваленцију, све формуле $\alpha(p_1, p_2, p_3)$ тако да буде:
(а) $p_1 \land \alpha \equiv p_1 \land p_2$ и $p_1 \lor \alpha \equiv p_1 \lor p_3$;
(б) $p_3 \Rightarrow \alpha \equiv p_3 \Rightarrow (p_1 \lor p_2)$ и $\alpha \Rightarrow p_3 \equiv \neg(p_1 \lor p_2) \Rightarrow p_3$;
(в) $p_1 \Rightarrow \alpha \equiv p_2 \Rightarrow (\neg p_1 \lor p_3)$ и $(p_3 \Rightarrow p_2) \Rightarrow p_1 \equiv \neg p_1 \Rightarrow \neg\alpha$
9. Одредити формулу $\alpha(p_1, p_2, p_3)$ која добија вредност 1 акко тачно два од слова p_1, p_2, p_3 добијају вредност 1.
10. Одредити формулу $\alpha(p_1, p_2, p_3)$ тако да је њена истинитосна вредност при било којој валуацији једнака вредности коју при тој валуацији добија већина слова p_1, p_2, p_3.
11. Одредити нормалне форме (кнф и днф) формуле:
(а) $((p_1 \Rightarrow p_2) \Rightarrow (p_3 \Rightarrow \neg p_1)) \Rightarrow (\neg p_2 \Rightarrow \neg p_3)$
(б) $\neg(p_1 \land (p_2 \lor p_3)) \Rightarrow ((p_1 \land p_2) \lor p_3)$
(в) $\neg(p \lor q) \land (p \Rightarrow r)$
(г) $(p \Leftrightarrow q) \land \neg(r \Rightarrow s)$
(д) $((p \Rightarrow q) \Leftrightarrow r) \land (p \lor \neg q)$
(ђ) $\neg((p \Leftrightarrow q) \Rightarrow (q \Leftrightarrow r))$

1. Математичка индукција

Када аритметику називам само једним делом логике, тиме већ исказујем да појам броја сматрам сасвим независним од представа или интуиција простора и времена, да га, напротив сматрам непосредним производом чистих закона мишљења.

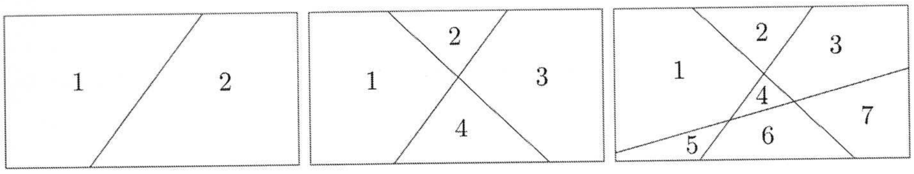
Рихард Дедекинд, цитат из чланка *Природа и значење бројева* (Was sind und was sollen die Zahlen), објављеног 1888. године

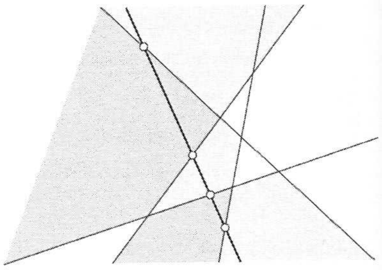
Рихард Дедекинд (1831–1916) био је немачки математичар. Дедекинд је дао велики допринос многим областима савремене математике. Посебно су значајни његови прилози аксиоматизацији аритметике и заснивању реалних бројева. Два Дедекиндова рада преведена су на многе језике и често заједно штампана као Есеји о теорији бројева: I Непрекидност и ирационални бројеви (1858) II Природа и значење бројева (1888). Чланак (I) је преведен у публикацији *Заснивање наставе математичке анализе*, Друштво математичара Србије (2019).

1.1. **Природни бројеви и принцип математичке индукције**

Увод. У равни је конструисано n правих тако да никоје две нису паралелне, нити се неке три секу у једној тачки. На колико области је подељена раван конструисаним правама?

Нека је A_n број области на које n конструисаних правих деле раван. Није тешко уочити: $A_0 = 1$, $A_1 = 2$, $A_2 = 4$, $A_3 = 7, \ldots$





Изводимо неколико општих закључака:

- Ако је нацртано n правих, нова права (конструисана тако да буду испуњени услови задатка) сече датих n правих у n тачака.
- Нова права је овим тачкама подељена на $n+1$ делова и сваки од тих делова се налази у једној од области на које n правих деле раван.
- Свака од тих $n+1$ области новом правом је подељена на две области.

Дакле, ако је нацртано n правих, цртањем нове праве број области се повећава за $n+1$: $A_{n+1} = A_n + (n+1)$.

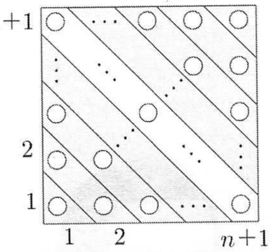
$$\begin{aligned} A_n &= A_{n-1} + n = A_{n-2} + (n-1) + n = \cdots = A_1 + 2 + \cdots + (n-1) + n \\ &= A_0 + 1 + 2 + \cdots + (n-1) + n \\ &= 1 + 1 + 2 + \cdots + (n-1) + n \end{aligned}$$

Једнакост $1 + 2 + \cdots + n = \dfrac{n \cdot (n+1)}{2}$, за било које $n \geqslant 1$, позната је од давнина. Узимајући у обзир ову формулу, добијамо да је

$$A_n = 1 + \frac{n \cdot (n+1)}{2} = \frac{n^2 + n + 2}{2}.$$

Питагорејци (старогрчки математичари, следбеници Питагоре) су збирове првих n природних бројева називали *троугаоним бројевима* и наведену једнакост су извели ослањајући се на слике.

Једнакост је $1 + 2 + \cdots + n = \dfrac{n \cdot (n+1)}{2}$, за $n \geqslant 1$, представља често први школски пример доказа математичком индукцијом.



Ако је $T_n = 1 + 2 + \cdots + n$, тј. T_n је n-ти троугаони број, на основу слике изнад једноставно уочавамо једнакости: $T_n + (n+1) + T_n = (n+1)^2$, тј. $T_n = \dfrac{n(n+1)}{2}$.

План

- бројање; индуктивне дефиниције сабирања, множења, степеновања
- принцип математичке индукције

Један од најзначајнијих производа људске мисли јесте *скуп* свих природних бројева 0, 1, 2, 3, 4, 5, 6, ... Бројање је једна од најзначајнијих вештина коју је човек стекао захваљујући свом чистом мишљењу, а не физичком раду.

Бројање је базични појам аритметике. Предмет аритметике нису бројеви већ бројање. Идеја бројања је на природан начин повезана са прадавним начином бележења резултата бројања у тзв. *рецка-систему*: записи резултата бројања настају тако што полазећи од 0 (почетног резултата који претходи бројању) узастопно дописујемо (једну по једну) цртицу: $0, 0', 0'', 0''', 0'''', \ldots$ или

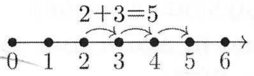
$$0, \overline{0}, \overline{\overline{0}}, \overline{\overline{\overline{0}}}, \overline{\overline{\overline{\overline{0}}}}, \ldots$$

У наставку, користимо овај други запис, при чему ћемо понекад користити и арапске цифре, да поједноставимо писање:

$$0, 1 = \overline{0}, 2 = \overline{\overline{0}}, 3 = \overline{\overline{\overline{0}}}, 4 = \overline{\overline{\overline{\overline{0}}}}, \ldots$$

Најважнији корак бележења резултата бројања јесте: *додавање нове цртице на текући резултат бројања.* На тај начин креирамо следбеника сваког броја. Нема никаквог ограничења: сваки број има свог следбеника.

Сабирање је операција која се природно надовезује на бројање: збир $m+n$ добијамо када почев од броја m избројимо још n бројева. Другим речима, збир $m+n$ је n-ти следбеник броја m. Сабирање се прецизно описује двема једнакостима:



$m + 0 = m$	[Када се броју m дода 0 резултат је m.]
$m + \overline{n} = \overline{m+n}$	[Ако је $m + n = k$, онда је $m + \overline{n} = \overline{k}$.]

Наведене једнакости описују како се (било ком) броју m додају природни бројеви, тј. дефинишу функцију којом се природном броју x додељује јединствен природан број $m + x$; ту функцију краће означавамо $x \mapsto m + x$. Сабирање је бројање почев од неког задатог броја. Нпр. збир $2 + 3$ (тј. $\overline{\overline{0}} + \overline{\overline{\overline{0}}}$) је трећи следбеник броја 2:

$$\begin{aligned} \overline{\overline{0}} + \overline{\overline{\overline{0}}} &= \overline{\overline{\overline{0}} + \overline{\overline{0}}} \\ &= \overline{\overline{\overline{\overline{0}} + \overline{0}}} \\ &= \overline{\overline{\overline{\overline{\overline{0}} + 0}}} \\ &= \overline{\overline{\overline{\overline{\overline{0}}}}} \end{aligned}$$

Користећи наведене једнакости изводимо општа својства сабирања. На пример, можемо ли доказати једнакост $0 + n = n$, за било који природан број n? Једноставно је проверити једнакост у било ком конкретном случају:

$0+0=0$ је последица једнакости $m+0=m$ коју иницијално претпостављамо за било који број m, па посебно и када је m једнако 0;

$0+\overline{0}=\overline{0+0}=\overline{0}$, јер је у претходном кораку показано $0+0=0$;

$0+\overline{\overline{0}}=\overline{0+\overline{0}}=\overline{\overline{0}}$, јер је у претходном кораку показано $0+\overline{0}=\overline{0}$;

$0+\overline{\overline{\overline{0}}}=\overline{0+\overline{\overline{0}}}=\overline{\overline{\overline{0}}}$, јер је у претходном кораку показано $0+\overline{\overline{0}}=\overline{\overline{0}}$;

⋮

У овом низу доказа примећујемо: осим за прву једнакост $0+0=0$, при доказивању сваке једнакости користимо једнакост која јој претходи. Када за неко n докажемо да је $0+n=n$, онда једноставно изводимо и следећу једнакост

$$0+\overline{n}=\overline{0+n}=\overline{n}.$$

Претходна запажања истичу суштину тзв. принципа математичке индукције.

$$\frac{\mathcal{S}(0), \mathcal{S}(0)\Rightarrow\mathcal{S}(1), \mathcal{S}(1)\Rightarrow\mathcal{S}(2), \ldots}{\mathcal{S}(0), \mathcal{S}(1), \mathcal{S}(2), \ldots}$$

Принцип математичке индукције: Нека је $\mathcal{S}$ ознака за неко својство природних бројева, и $\mathcal{S}(n)$ ознака да *број n има својство* $\mathcal{S}$. Из следећа два услова:

БИ (База индукције)
0 има својство $\mathcal{S}$, тј. $\mathcal{S}(0)$;

ИК (Индуктивни корак)
за свако n, ако n има својство $\mathcal{S}$, онда и $\overline{n}$ има својство $\mathcal{S}$, тј. $\mathcal{S}(n)\Rightarrow\mathcal{S}(\overline{n})$;

закључујемо да сваки природни број има својство $\mathcal{S}$.

Индуктивни корак заправо представља доказ да операција *следбеник* чува уочено својство.

Теорема 4. *За сваки природан број n, $0+n=n$.*

Доказ. Сабирање је дефинисано двема једнакостима:

$$\begin{aligned}&(\mathrm{Rec1})\ m+0=m\\&(\mathrm{Rec2})\ m+\overline{n}=\overline{m+n}\end{aligned}$$

Једнакост $0+n=n$ посматрамо као $\mathcal{S}(n)$ из принципа математичке индукције.
(БИ) Да ли важи $\mathcal{S}(0)$, тј. $0+0=0$? Ова једнакост директно следи из (Rec1).
(ИК) Да ли, за произвољно n важи $\mathcal{S}(n)\Rightarrow\mathcal{S}(\overline{n})$? Другим речима, да ли из претпоставке да је $0+n=n$ можемо извести једнакост $0+\overline{n}=\overline{n}$?

Уводимо тзв. индуктивну претпоставку: Нека је n природан број такав да је $0+n=n$. Применом ове претпоставке и (Rec2) долазимо до жељене једнакости:

$$\begin{aligned}0+\overline{n} &= \overline{0+n} \text{ према (Rec2)}\\ &= \overline{n} \text{ према индуктивној претпоставци}\end{aligned}$$

Дакле, према принципу математичке индукције, за сваки природан број n тачна је једнакост $0 + n = n$. □

Теорема 5. *За све природне бројеве m, n, k важе једнакости:*

(1) $m + (n + k) = (m + n) + k$

(2) $\overline{m} + n = m + \overline{n}$;

(3) $m + n = n + m$;

Доказ. (1) Индукцијом по k:
(БИ) Једноставно се доказује једнакост $(m+n)+0 = m+(n+0)$.
(ИП) $(m+n)+k = m+(n+k)$

$$
\begin{aligned}
(m+n)+\overline{k} &= \overline{(m+n)+k} && \text{[према (Rec2)]}\\
&= \overline{m+(n+k)} && \text{[према ИП]}\\
&= m+\overline{n+k} && \text{[према (Rec2)]}\\
&= m+(n+\overline{k}) && \text{[према (Rec2)]}
\end{aligned}
$$

(2) Индукцијом по n:

$$
\begin{aligned}
\text{(БИ)}\quad \overline{m}+0 &= \overline{m} && \text{[према (Rec1)]}\\
&= \overline{m+0} && \text{[према (Rec1)]}\\
&= m+\overline{0} && \text{[према (Rec2)]}
\end{aligned}
$$

(ИП) $\overline{m}+n = m+\overline{n}$

$$
\begin{aligned}
\overline{m}+\overline{n} &= \overline{\overline{m}+n} && \text{[према (Rec2)]}\\
&= \overline{m+\overline{n}} && \text{[према ИП]}\\
&= m+\overline{\overline{n}} && \text{[према (Rec2)]}
\end{aligned}
$$

(3) Индукцијом по n:
(БИ) Из $m+0=m$ и $0+m=m$ следи да је $m+0=0+m$.
(ИП) $m+n=n+m$

$$
\begin{aligned}
m+\overline{n} &= \overline{m+n} && \text{[према (Rec2)]}\\
&= \overline{n+m} && \text{[према ИП]}\\
&= n+\overline{m} && \text{[према (Rec2)]}\\
&= \overline{n}+m && \text{[према (1)]}
\end{aligned}
$$

□

Због асоцијативности сабирања, $m + (n + k) = (m + n) + k$, кратко пишемо $m + n + k$ остављајући могућност да се по потреби додају заграде које обухватају први и други сабирак, или заграде које обухватају други и трећи сабирак.

На сличан начин, као сабирање, уводимо и **множење**, прецизирајући познату „интуитивну” једнакост: $m \cdot n = \underbrace{m + \cdots + m}_{n \text{ пута}}$.

Множење описујемо следећим двема једнакостима:

$$
\begin{aligned}
m \cdot 0 &= 0\\
m \cdot \overline{n} &= (m \cdot n) + m
\end{aligned}
$$

Према знаном договору да је множење приоритетније од сабирања, уместо $(m \cdot n) + m$, краће пишемо $m \cdot n + m$.

Теорема 6. *За све природне бројеве m, n, k важе једнакости:*

(1) $k \cdot (m + n) = k \cdot m + k \cdot n$

(2) $(k \cdot m) \cdot n = k \cdot (m \cdot n)$

(3) $0 \cdot n = 0$

(4) $\overline{m} \cdot n = m \cdot n + n$

(5) $m \cdot n = n \cdot m$

Доказ. (1) Индукцијом по n:
(БИ) Из $k \cdot (m+0) = k \cdot m$ и $k \cdot m + k \cdot 0 = k \cdot m + 0 = k \cdot m$ следи да је $k \cdot (m+0) = k \cdot m + k \cdot 0$.
(ИП) $k \cdot (m+n) = k \cdot m + k \cdot n$

$$\begin{aligned} k \cdot (m + \overline{n}) &= k \cdot \overline{m+n} \\ &= k \cdot (m+n) + k \\ &= (k \cdot m + k \cdot n) + k \quad \text{[према ИП]} \\ &= k \cdot m + (k \cdot n + k) \\ &= k \cdot m + k \cdot \overline{n} \end{aligned}$$

(4) Индукцијом по n:
(БИ) Једноставно се уочава да је једнакост $\overline{m} \cdot 0 = m \cdot 0 + 0$ тачна.
(ИП) $\overline{m} \cdot n = m \cdot n + n$

$$\begin{aligned} \overline{m} \cdot \overline{n} &= \overline{m} \cdot n + \overline{m} \\ &= (m \cdot n + n) + \overline{m} \quad \text{[према ИП]} \\ &= m \cdot n + (n + \overline{m}) \\ &= m \cdot n + (\overline{n} + m) \\ &= m \cdot n + (m + \overline{n}) \\ &= (m \cdot n + m) + \overline{n} \\ &= m \cdot \overline{n} + \overline{n} \end{aligned}$$

Остале једнакости остављамо за вежбу. □

Начин на који смо увели сабирање и множење називамо **индуктивним**, одн. **рекурзивним** или **рекурентним** дефиницијама. Индуктивним дефиницијама уводимо веома богату класу аритметичких операција. У наставку, прелазимо на ознаке које су уобичајене у литератури, и уместо $\overline{n}$ пишемо $n+1$. (Приметите да је $n + 1 = n + \overline{0} = \overline{n+0} = \overline{n}$.)

Реч рекурзија потиче од латинске речи recurrere која значи *вратити се од* [recurrence – који се враћа]. Дедекинд је у свом раду из 1888. користио термин *дефинисан индукцијом*, док је Хилберт (1904) употребио реч rekurrent(e), а касније (1923) и реч Rekursion.

Степеновање:[33]

$$\begin{cases} m^0 = 1 \\ m^{n+1} = m^n \cdot m \end{cases}$$

Факторијел:[34]

$$\begin{cases} 0! = 1 \\ (m+1)! = m! \cdot (m+1) \end{cases}$$

Биномни коефицијенти $\binom{\cdot}{2}$**:**

$$\begin{cases} \binom{0}{2} = 0 \\ \binom{m+1}{2} = \binom{m}{2} + m \end{cases}$$

Из принципа математичке индукције се изводе разне специјалне врсте индукције прилагођене неким специфичним применама. Наводимо неколико таквих примера. Нека је $\mathcal{S}$ неко својство природних бројева.

[33] $m^n = \underbrace{m \cdot \ldots \cdot m}_{n \text{ пута}}$

[34] $m! = 1 \cdot 2 \cdot \ldots \cdot m$

Принцип математичке индукције са две хипотезе: Сваки природан број има својство $\mathcal{S}$, ако важе следећа два услова:

БИ (База индукције)
0 и 1 имају својство $\mathcal{S}$, тј. $\mathcal{S}(0) \wedge \mathcal{S}(1)$;

ИК (Индуктивни корак)
за свако n, ако n и $n+1$ имају својство $\mathcal{S}$, онда и $n+2$ има својство $\mathcal{S}$, тј. $\mathcal{S}(n) \wedge \mathcal{S}(n+1) \Rightarrow \mathcal{S}(n+2)$.

Принцип потпуне математичке индукције: Сваки природан број има својство $\mathcal{S}$, ако важе следећа два услова:

БИ (База индукције)
0 има својство $\mathcal{S}$, тј. $\mathcal{S}(0)$;

ИК (Индуктивни корак)
за свако n, ако бројеви $0, \ldots, n$ имају својство $\mathcal{S}$, онда и $n+1$ има својство $\mathcal{S}$, тј. $\mathcal{S}(0) \wedge \cdots \wedge \mathcal{S}(n) \Rightarrow \mathcal{S}(n+1)$.

Чувени француски математичар Анри Поенкаре (1854–1912) своју књигу La Science et l'Hypothèse[35] почиње рекурентним дефиницијама основних рачунских операција и доказима основних аритметичких својстава. Напослетку, истиче: *Наведени докази аритметичких тврђења илуструју математичко резоновање par excellence*[36]*, и морамо га ближе проучити.* Ово par excellence резоновање биће примењено на неке нове ситуације и представљаће основу свих разматрања у овом поглављу.

[35] Наука и хипотеза

[36] par excellence (пар екселâнс) је француски израз који се користи у многим језицима да означи *нај-бољи, прави пример нечега.*

▼ Задаци и додаци

Принцип рекурзије	Принцип индукције
метод за **дефинисање** низа елемената неког скупа: $S_0, S_1, S_2, \ldots, S_n, S_{n+1}, \ldots$	метод за **доказивање** низа тврђења: $\mathcal{S}(0), \mathcal{S}(1), \mathcal{S}(2), \ldots, \mathcal{S}(n), \mathcal{S}(n+1), \ldots$
- S_0 је дефинисано ($S_0 = x$, где је x неки фиксиран елемент задатог скупа); - елемент S_{n+1} је дефинисан у зависности од n и S_n, тј. за сваки природан број n дата је веза између S_{n+1} и S_n облика $S_{n+1} = F(n, S_n)$.	(БИ) $\mathcal{S}(0)$ је тачно; (ИК) истинитост исказа $\mathcal{S}(n+1)$ се доказује из претпоставке $\mathcal{S}(n)$, тј. доказује се да за сваки природан број n важи импликација: $\mathcal{S}(n) \Rightarrow \mathcal{S}(n+1)$.
Пример 1.	
Дат је низ бројева: $f_1 = 5$, $f_{n+1} = 5 + f_n$, $n \in \mathbb{N}$. Одредити f_5.	Доказати да за сваки природан број n, $5 \mid f_n$.

1. (а) Доказати да се сваки природан број $n \geqslant 8$ може приказати као збир тројки и петица, тј. у облику $n = 3k + 5\ell$, за неке $k, \ell \geqslant 0$.

(б) Доказати да се сваки природан број $n \geqslant 24$ може приказати као збир петица и седмица, тј. у облику $n = 5k + 7\ell$, за неке $k, \ell \geqslant 0$.
(в) Доказати да се сваки природан број $n \geqslant 14$ може приказати као збир тројки и осмица, тј. у облику $n = 3k + 8\ell$, за неке $k, \ell \geqslant 0$.
2. Низ је рекурзивно дефинисан: $a_0 = 0$, $a_{n+1} = a_n + 2(n+1)$, $n \geqslant 0$. Доказати да је $a_n = n(n+1)$, за свако n.
3. Низ је рекурзивно дефинисан: $a_0 = 1$, $a_{n+1} = 2a_n + 1$, $n \geqslant 0$. Доказати да је $a_n + 1 = 2^n$, за свако n.
4. Низ је рекурзивно дефинисан: $g_0 = 1$, $g_{n+1} = g_n + 3^{n+1}$, $n \geqslant 0$. Доказати да је $2g_n + 1 = 3^n$, за свако n.
5. Низ је рекурзивно дефинисан:

$$S_0 = 0,\, S_{n+1} = S_n + (n+1)! \cdot (n+1), n \geqslant 0.$$

Доказати да је $S_n + 1 = (n+1)!$, за свако n.
6. Доказати да су сви чланови низа

$$b_0 = 1007, b_1 = 10017, b_2 = 100117, \ldots, b_n = 10011 \cdots 17, \ldots$$

дељиви са 53.
Упутство. Најпре треба уочити како се сваки члан низа, почев од другог, добија из претходног, тј. описати везу између b_n и b_{n+1}: $b_{n+1} = (b_n - 6) \cdot 10 + 7 = 10b_n - 53$.

Дељењем се уверавамо да тврђење важи за првих неколико чланова:
$1007 : 53 = 19$
$10017 : 53 = 189$
$100117 : 53 = 1889$
$1001117 : 53 = 18889, \ldots$

7. Доказати да су сви чланови низа $12008, 120308, 1203308, 12033308, 120333308, \ldots$ дељиви са 19.
8. [38] Робот може да изврши следеће три команде:
F – направи јединични корак напред;
L – окрени се улево за 90°;
R – окрени се удесно за 90°.

Програм је низ команди. Посматрамо само посебне програме P_n, $n \geqslant 0$. Основни програм P_0 садржи само једну команду F. Програм P_{n+1} (за $n \geqslant 0$) започиње програмом P_n, окретом улево за 90°, још једним понављањем програма P_n и најзад окретом удесно за 90°; односно $P_{n+1} = P_n\mathtt{L}P_n\mathtt{R}$. На пример, $P_1 = \mathtt{FLFR}$.
(а) Написати програм P_2.
(б) Колики пут ће прећи робот извршавајући програм P_n? Другим речима, колико команди F садржи програм P_n?
(в) Нека је ℓ_n укупан број команди у P_n; нпр. $\ell_0 = 1$, $\ell_1 = 4$. Формулом изразити везу између ℓ_{n+1} и ℓ_n. Изразити ℓ_n у зависности од n.
(г) У почетном положају робот се налази у координатном почетку и окренут је у позитивном смеру x-осе. У ком смеру је окренут робот након извршавања програма P_n?
(д) Нацртати путању робота у координатном систему, ако се он на почетку налази као што је описано под (г).
(ђ) Нека је (x_n, y_n) позиција робота након извршавања програма P_n; нпр. $(x_0, y_0) = (1, 0)$, $(x_1, y_1) = (1, 1)$. Истражити везу између (x_{n+1}, y_{n+1}) и (x_n, y_n). Одредити (x_8, y_8). Одредити (x_{8k}, y_{8k}).

[38] Maths Admissions Test, Oxford University, 2012

9. Низ формула $\alpha_1, \alpha_1, \alpha_3, \ldots$ дефинисан је индуктивно:[39]

$$\begin{array}{lll} \alpha_1 & \text{је формула} & p \Rightarrow q_1 \\ \alpha_{n+1} & \text{је формула} & \alpha_n \wedge (q_n \Rightarrow q_{n+1}),\ n \geqslant 1 \end{array}$$

Доказати да је за свако $n \geqslant 1$, формула $\alpha_n \Rightarrow (p \Rightarrow q_n)$ таутологија.

[39] Очигледно, за свако $n \geqslant 1$, у формули α_n се појављују само исказна слова $p, q_1, \ldots, q_n$.

10. Низ формула $\alpha_1, \alpha_1, \alpha_3, \ldots$ дефинисан је индуктивно:

$$\begin{array}{lll} \alpha_1 & \text{је формула} & p \Rightarrow p_0 \\ \alpha_{n+1} & \text{је формула} & \alpha_n \wedge (p_n \Rightarrow p_{n+1}),\ n \geqslant 1 \end{array}$$

Доказати да је за свако $n \geqslant 1$, формула $\neg p_n \wedge \alpha_n \Rightarrow \neg p$ таутологија.

11. Низ формула $\alpha_1, \alpha_1, \alpha_3, \ldots$ дефинисан је индуктивно:

$$\begin{array}{lll} \alpha_1 & \text{је формула} & p_1 \\ \alpha_{n+1} & \text{је формула} & \alpha_n \Leftrightarrow p_{n+1},\ n \geqslant 1 \end{array}$$

Доказати да за свако $n \geqslant 1$ и произвољну валуацију v, валуација v задовољава формулу α_n акко v додељује вредност 0 непарном броју слова која се појављују у α_n.

12. Низ формула $\alpha_1, \alpha_1, \alpha_3, \ldots$ дефинисан је индуктивно:

$$\begin{array}{lll} \alpha_1 & \text{је формула} & p \\ \alpha_{n+1} & \text{је формула} & \alpha_n \Leftrightarrow p,\ n \geqslant 1 \end{array}$$

Доказати да је α_n таутологија акко је n паран број.

Додатак

Скуп исказних формула је *индуктивно дефинисан*. Најпре су уведене најједноставније исказне формуле:

- свако исказно слово и свака логичка константа јесте исказна формула.

Затим је прецизирано како се формирају сложеније исказне формуле:

- Ако је α исказна формула, онда је и $\neg\alpha$ исказна формула;
- ако су α и β исказне формуле, онда су и $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \Rightarrow \beta)$, $(\alpha \Leftrightarrow \beta)$ исказне формуле.

У складу са овом индуктивном дефиницијом, спроводимо тзв. доказе *индукцијом по сложености формуле.* Да бисмо доказали да неко својство важи за све изказне формуле, најпре доказујемо базу индукције:

(БИ) свако исказно слово и свака логичка константа задовољавају тражено својство,

а затим и индуктивни корак, тј. да својство важи и за сложеније формуле, под претпоставком да важи за једноставније од којих је та формула састављена:

(ИК) ако α задовољава тражено својство, онда и $\neg\alpha$ задовољава тражено својство;
ако α и β задовољавају тражено својство, онда и $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \Rightarrow \beta)$, $(\alpha \Leftrightarrow \beta)$ задовољавају то исто својство.

---

13. Доказати да за сваку формулу α,

$$\alpha \equiv (\alpha[p/\bot] \wedge \neg p) \vee (\alpha[p/\top] \wedge p).$$

14. За формулу кажемо да је *позитивна* ако је исказно слово или је сложенија формула у којој се појављују само везници $\wedge$ и $\vee$:

- исказна слова су позитивне формуле;
- ако су α и β позитивне формуле, онда су то и $(\alpha \wedge \beta)$ и $(\alpha \vee \beta)$.

(а) Доказати да ниједна позитивна формула није таутологија.

(б) Доказати да је свака позитивна формула задовољива.

15. Исказне формуле које су изграђене од исказних слова $p_1, p_2, p_3, \ldots$ и везника $\neg, \wedge, \vee$ називаћемо *једноставним* формулама:

- исказна слова су једноставне формуле;
- ако је α једноставна формула, онда је и $\neg\alpha$ једноставна формула;
- ако су α и β једноставне формуле, онда су то и $(\alpha \wedge \beta)$ и $(\alpha \vee \beta)$.

Ако је α једноставна формула, нека је α^* формула добијена заменом сваког исказног слова p_i формулом $\neg p_i$, и заменом везника $\wedge$ и $\vee$ редом везницима $\vee$ и $\wedge$. Ова трансформација се индуктивно дефинише на следећи начин:

- $p_i^* = \neg p_i$;
- $(\neg\alpha)^* = \neg\alpha^*$;
- $(\alpha \wedge \beta)^* = \alpha^* \vee \beta^*$; $(\alpha \vee \beta)^* = \alpha^* \wedge \beta^*$.

Доказати да за сваку једноставну формулу α, $\neg\alpha \equiv \alpha^*$.

16. Имајући у виду значење формуле $(\alpha \wedge \beta) \vee (\neg\alpha \wedge \gamma)$ можемо је записати и у облику if-формуле: $\text{if}\,\alpha\,\text{then}\,\beta\,\text{else}\,\gamma$. Скуп if-формула дефинишемо као најмањи скуп такав да важи:

- исказна слова и логичке константе $\top$ и $\bot$ су if-формуле,
- ако су α, β и γ if-формуле, онда је $\text{if}\,\alpha\,\text{then}\,\beta\,\text{else}\,\gamma$ такође if-формула.

(а) Доказати да је свака исказна формула еквивалентна некој if-формули.

(б) Доказати да су еквивалентне следеће формуле

$$\text{if (if } p \text{ then } q \text{ else } r) \text{ then } q_1 \text{ else } r_1$$

и

$$\text{if } p \text{ then (if } q \text{ then } q_1 \text{ else } r_1) \text{ else (if } r \text{ then } q_1 \text{ else } r_1).$$

(в) Кажемо да је if-формула *проста* уколико је услов (формула која се налази између if и then) исказно слово. Доказати да је свака if-формула еквивалентна некој простој if-формули.

(г) Кажемо да је if-формула *нормална* ако је проста и ако су све њене if-потформуле облика $\text{if}\,p\,\text{then}\,\alpha\,\text{else}\,\beta$, при чему је p исказно слово које се не појављује ни у α нити у β. Доказати да је свака if-формула еквивалентна некој нормалној if-формули.

1.2 Формалне граматике и формалне теорије

Увод. Наводимо неколико правила[40] која дефинишу један фрагмент граматике енглеског језика.

[40] Пример је преузет са такмичења NACLO (North American Computational Linguistics Olympiad) 2009

(1) Sentence → NounPhrase Verb NounPhrase
(2) NounPhrase → Noun (3) NounPhrase → Adjective NounPhrase
(4) Noun → people (5) Verb → love
(6) Adjective → good (7) Adjective → charming (8) Adjective → happy
(9) Adjective → bad (10) Adjective → obnoxious (11) Adjective → unhappy

Правило (1) описује како састављамо Sentence: најпре наводимо NounPhrase, затим размак, па Verb, још један размак и најзад NounPhrase. Правила (2) и (3) описују две могућности да се састави NounPhrase: то може бити само Noun, или се саставља тако што се на Adjective надовеже размак и нека друга NounPhrase. Преостала правила (4–11) представљају речник, који садржи једну именицу Noun (4), један глагол Verb (5) и шест придева Adjectives (6–11). Изведимо једну реченицу:

Sentence → NounPhrase Verb NounPhrase
→ Adjective NounPhrase Verb NounPhrase
→ Adjective Noun Verb NounPhrase
→ Adjective Noun Verb Adjective NounPhrase
→ Adjective Noun Verb Adjective Adjective NounPhrase
→ Adjective Noun Verb Adjective Adjective Noun
→ ⋮
→ happy people love bad charming people

Према принципу 'супротности се привлаче', *тачним* се сматрају само оне реченице којима се тврди да особе са искључиво позитивним особинама (good, charming, happy) воле особе са искључиво негативним особинама (bad, obnoxious, unhappy), и обратно, особе са негативним особинама воле особе са позитивним особинама. На пример, тачне су реченице:

- good happy people love obnoxious people
- obnoxious people love good good happy people

Али, *лажне* су следеће реченице:

- good people love good people
- people love good people
- charming bad people love unhappy good people

Саставити по узору на дати фрагмент граматике, правила за састављање само тачних реченица TrueSentence.

План

- алфабет, реч, правило трансформације, Туов процес
- проблем описивања свих речи које се могу добити Туовим процесом
- формална граматика: помоћни и крајњи симболи, почетни симбол
- језик одређен формалном граматиком
- формалне теорије: алфабет, формуле, аксиоме, правила извођења
- извођење у формалној теорији; извођење из хипотеза

Чувени амерички лингвиста Ноам Чомски (1928-) је принцип индуктивног (рекурзивног) дефинисања препознао и као темељни принцип језичке структуре. Ова чињеница лежи у основи развоја вештачких (формалних) језика међу којима се посебно значајно место заузимају програмски језици. Полазимо од основних појмова на којима почива изградња сваког формалног језика.

Основне идеје овог одељка потичу од Емила Поста (1897–1954), америчког математичара. Шта год да представљају *изрази* неког логичког система, одн. језика, они се у крајње уопштеној анализи своде на *низове симбола неког коначног алфабета.* Веома сложени логички и математички системи засновани су на правилима која одређују како се неки низови симбола могу трансформисати у неке друге низове симбола.

▼ Алфабет

Полазиште у развоју било ког формалног језика представља избор **алфабета**. Уопштено, под *алфабетом* Σ подразумевамо било који непразан коначан скуп чије елементе називамо *симболима*. Сваки алфабет користимо да бисмо написали неки текст. Наводимо неколико познатих алфабета:

- $\Sigma_{\text{U}} = \{|\}$ – *унарни алфабет*, који садржи само један симбол;
- $\Sigma_2 = \{0, 1\}$ – *бинарни алфабет*, веома важан за рачунарство;
- $\Sigma_{\text{keyboard}} = \{\mathtt{A}, \mathtt{a}, \mathtt{B}, \mathtt{b}, \ldots, \mathtt{Z}, \mathtt{z}, \sqcup, >, <, (,), \ldots, !\}$ – алфабет свих симбола тастатуре (при чему $\sqcup$ означава бланко знак); итд.

▼ Речи

Ако је Σ алфабет, **реч** је коначан низ надовезаних симбола из Σ. Број надовезаних симбола једне речи је *дужина те речи*; дужину речи w обележавамо $|w|$. За $m \geqslant 2$, Σ^m је скуп свих речи дужине m. Скуп Σ^1, тј. скуп свих речи над Σ дужине 1, идентификујемо са скупом Σ. Скуп Σ^0 је једночлани скуп чији ћемо елемент означавати са ε и при томе ћемо сматрати да је и ε реч над Σ и то *празна реч*. Скуп свих речи над алфабетом Σ означавамо Σ^*. Да бисмо поједноставили записивање, узастопна понављања истог симбола $\underbrace{aa\cdots a}_{n \text{ пута}}$ краће записујемо a^n; специјално a^0 је празна реч.

Треба приметити да термин *реч*, који овде користимо има другачије значење него у говорном језику. У значењу које овде уводимо, реч може бити веома дугачак низ симбола, без неког посебног значења.
$\Sigma_2^0 = \{\varepsilon\}$, $\Sigma_2^1 = \{0, 1\}$,
$\Sigma_2^2 = \{00, 01, 10, 11\}$,
$\vdots$
$\Sigma_2^* = \{\varepsilon, 0, 1, 00, 01, 10, \ldots\}$
Приметимо да ако алфабет Σ садржи k симбола, онда скуп Σ^m садржи k^m речи.

▼ Правила за трансформацију речи

Развој *рачуна* са речима данас заузима значајно место у алгебри, логици, геометрији, рачунарству. Основу свих тих рачуна чине правила за трансформације речи која су у суштини заснована на идеји супституције. Сваки пар речи u и w, над неким алфабетом Σ, одређује *правило* које се означава $u \to w$ (или $[u/w]$). Правило $u \to w$ можемо применити на сваку реч v која садржи u као подреч, тј. на реч v облика v_1uv_2, за неке (можда празне) речи v_1 и v_2. Примена правила подразумева да подреч u заменимо речју w; пишемо: $v_1uv_2 \to v_1wv_2$. Дозвољена су и правила следећег облика:

- $u \to \varepsilon$, тј. брисање подречи u;
- $\varepsilon \to v$, тј. уметање речи v на било ком месту.

▼ Семи-Туов процес

Када је задат неки коначан скуп правила, кажемо да се из v **изводи** реч v', ако постоји коначан низ речи

$$v = v_0 \to v_1 \to v_2 \to \cdots \to v'$$

такав да је свака реч, почевши од друге, добијена применом неког

од правила на реч која јој претходи.

Скуп правила за трансформацију речи задатог алфабета назива се *Семи-Туов процес* или *систем преписивања* над тим алфабетом.

Аксел Туе (1863–1922) је био норвешки математичар, по коме се често зову системи правила за трансформисање речи.

Пример 13. Семи-Туов процес над алфабетом $\Sigma = \{a, b\}$ је одређен правилима: $ab \to aa$ и $ba \to bb$. Ево једног извођења речи aaa из aba:

$$aba \to abb \to aab \to aaa$$

Може ли се, применом датих правила, из $aaabb$ извести $aaaaa$? Може ли се из $aaabb$ извести $bbbbb$?

У свакој речи, подреч ab можемо заменити са aa, а подреч ba можемо заменити са bb.

▼ Језик одређен формалном граматиком

Формална граматика је посебна врста система преписивања који је одређен:

- алфабетом у коме се разликују две врсте симбола:
  - *помоћни симболи*[45], при чему је један од њих посебно издвојен као тзв. *почетни симбол* и
  - *крајњи симболи* – тзв. *терминали*.
- коначним списком правила са чије се леве стране налази бар један помоћни симбол.

[45] У теорији формалних граматика, помоћни симболи често се називају и *промењиве*, али ми нећемо користити тај термин, јер ћемо реч *промењива* много више употребљавати у другачијем контексту.

Језик одређен формалном граматиком јесте скуп свих речи састављених од терминала које се могу извести из полазног симбола.

Пример 14. Над алфабетом $\{\mathsf{S}, a, b\}$, где је S полазни симбол, а a, b терминали, дата су правила

$$\mathsf{S} \to a\mathsf{S} \qquad \mathsf{S} \to b$$

Да бисмо описали језик одређен овом граматиком, важно је истражити какве се речи могу извести из полазног симбола S.

Пример илуструје две важне примене принципа математичке индукције, које ћемо често примењивати проучавајући разне формалне системе: индукцију по сложености речи и индукцију по дужини доказа.

Није тешко уочити да се из S могу извести речи $a^n b$ или $a^n\mathsf{S}$, за било које $n \geqslant 0$. Доказ ове чињенице спроводимо индукцијом по n.

БИ $n = 0$: јасно је да се из S могу извести речи b (директном применом правила $\mathsf{S} \to b$) и S (без примене иједног правила).

ИК Претпоставимо да се за неко n, из S могу извести $a^n b$ и $a^n\mathsf{S}$. Покажимо да се могу извести и речи $a^{n+1}b$ и $a^{n+1}\mathsf{S}$; обе ове речи се добијају из $a^n\mathsf{S}$ применом одговарајућих правила. Извођење речи $a^{n+1}\mathsf{S}$:

$$\begin{array}{lll} \mathsf{S} & \to a^n\mathsf{S} & [\text{према ИП}] \\ & \to a^n a\mathsf{S} & [\text{применом } \mathsf{S} \to a\mathsf{S}] \end{array}$$

Извођење речи $a^{n+1}b$:

$$\begin{array}{lll} \mathsf{S} & \to a^n\mathsf{S} & [\text{према ИП}] \\ & \to a^n a\mathsf{S} & [\text{применом } \mathsf{S} \to a\mathsf{S}] \\ & \to a^n ab & [\text{применом } \mathsf{S} \to b] \end{array}$$

Докажимо и да се из S могу извести **само** речи облика $a^n\mathsf{S}$ или $a^n b$, $n \geqslant 0$. Другим речима, ако је w реч која се може извести из S, треба доказати да је w облика $a^n\mathsf{S}$ или $a^n b$, $n \geqslant 0$. Доказ спроводимо **индукцијом по дужини извођења**.

БИ Ако је дужина извођења речи w из S једнака 0, тј. ниједно правило није примењено, онда је w заправо реч S, тј. реч $a^0\mathsf{S}$.

ИП Претпоставимо да тврђење важи за све речи дужине мање од k, за неки природан број $k \geqslant 1$. Докажимо да важи и за извођење дужине k.

Претпоставимо да је дужина извођења речи w из S једнака k:

$$\underbrace{\mathsf{S} \to \cdots \to w'}_{k-1 \text{ корака}} \to w$$

при чему је w' реч која се добија у претпоследњем кораку извођења. Према индуктивној претпоставци, w' је облика $a^n b$ или $a^n\mathsf{S}$.

Међутим, реч w' не може бити облика $a^n b$, јер ова реч не садржи S и на њу се не може применити ниједно од датих правила. Дакле, w' је облика $a^n\mathsf{S}$. Ако је последње примењено $\mathsf{S} \to a\mathsf{S}$, добијамо да је w облика $a^{n+1}\mathsf{S}$. Ако је последње примењено правило $\mathsf{S} \to b$, добијамо да је w облика $a^n b$.

Закључујемо да језик дате граматике чине само речи облика $a^n b$, $n \geqslant 0$.

Полазни симбол, у извесном смислу репрезентује сам језик, тј. скуп свих речи над терминалима које се могу извести из полазног симбола. То важно запажање илуструјемо у наредним примерима.

Пример 15. Палиндром је реч која се једнако чита и слева надесно и здесна налево. Палиндроми над $\{0,1\}$ су: 0, 010, 010010, итд. Наравно, и празна реч је палиндром. Скуп P **свих** палиндрома (укључујући и празну реч) над $\{0,1\}$ индуктивно дефинишемо на следећи начин:

- ε, 0 и 1 су палиндроми ($\varepsilon, 0, 1 \in P$);
- ако је w палиндром, онда су то и $0w0$ и $1w1$ (ако $w \in P$, онда $0w0, 1w1 \in P$).

Подсећамо, ε је празна реч.

Овој индуктивној дефиницији у потпуности одговарају следећа правила над алфабетом $\{P, 0, 1\}$, где је P полазни симбол, а 0 и 1 терминали:

$$P \to \varepsilon \qquad P \to 0 \quad P \to 1 \quad P \to 0P0 \quad P \to 1P1$$

Полазећи од симбола P можемо извести било који палиндром. Изведимо, на пример 0010100:

$$\begin{array}{lll} P & \to 0P0 & [\text{применом } P \to 0P0] \\ & \to 00P00 & [\text{применом } P \to 0P0] \\ & \to 001P100 & [\text{применом } P \to 1P1] \\ & \to 0010100 & [\text{применом } P \to 0] \end{array}$$

Штавише, палиндроми су једине речи над $\{0,1\}$ које се могу извести из P.

Пример 16. Посматрајмо правила над алфабетом $\{I,+,-,0,1,x,y,z,(,)\}$, где је I полазни симбол, а остали симболи су терминали:

$$I \to x \quad I \to y \quad I \to z \quad I \to 0 \quad I \to 1 \quad I \to -I \quad I \to (I+I)$$

Будући да сва правила са леве стране имају исти симбол I, све заједно их краће записујемо на следећи начин:

$$(*) \quad I \to x \mid y \mid z \mid 0 \mid 1 \mid -I \mid (I+I).$$

Није тешко уочити да из симбола I можемо извести било који израз у коме се појављују променљиве x, y или z, константе 0 или 1, знак за сабирање, и знак за супротни број, уз уобичајену употребу заграда. Изведимо, на пример, израз $-(1+x)$:

$$\begin{array}{lll} I & \to -I & [\text{применом } I \to -I] \\ & \to -(I+I) & [\text{применом } I \to (I+I)] \\ & \to -(1+I) & [\text{применом } I \to 1] \\ & \to -(1+x) & [\text{применом } I \to x] \end{array}$$

Ово извођење можемо посматрати и као доказ да је $-(1+x)$ заиста израз по (одговарајућој индуктивној) дефиницији.

Списак наведених правила прати следећу индуктивну дефиницију скупа I свих израза наведеног облика:

- $x, y, z, 0, 1$ су (најједноставнији) изрази, тј. $x,y,z,0,1 \in I$;
- ако је α израз, онда је и $-\alpha$ израз, тј. ако $\alpha \in I$, онда и $-\alpha \in I$;
- ако су α и β изрази, онда је $(\alpha+\beta)$ израз, тј. ако $\alpha,\beta \in I$, онда и $(\alpha+\beta) \in I$.

Пример 17. Уобичајено је да приликом изградње израза имамо неограничено много променљивих на располагању, тј. да за променљиве користимо слова са индексима; нпр. $v_0, v_1, v_2, v_3, v_4, \ldots$ За записивање природних бројева довољна су два симбола: симбол за први природан број и симбол за дописивање којим се од једног природног броја добија његов следбеник. Ако за те потребе изаберемо симболе v и $/$, добијамо: v, $v/$, $v//$, $v///$ итд. Проширујући алфабет симболима, P, v, $/$, где је P помоћни симбол, користећи правила

$$P \to v, \quad P \to P/$$

из P изводимо речи: v, $v/$, $v//, v///, \ldots$ које ћемо редом једноставније означавати $v, v_1, v_2, v_3, \ldots$ и називати их променљивама. Ако овако одређене променљиве, заједно са симболима 0 и 1, користимо као најједноставније изразе, а сложеније изразе градимо, као у претходном примеру, користећи знаке операција $+$ и $-$, и заграде, правила одговарајуће граматике, са полазним симболом I су:

$$I \to P \mid 0 \mid 1 \mid -I \mid (I+I), \qquad P \to v \mid P/$$

На пример, из I се изводи израз $-(v_3+(-v_2+0))$.

Пример 18. Над алфабетом $\{F,P,\Rightarrow,\neg,\top,\bot,p,/,(,)\}$ посматрамо следећа правила:

$P \to p \quad P \to P/$
$F \to \top \quad F \to \bot \quad F \to P \quad F \to \neg F \quad F \to (F \Rightarrow F)$

Није тешко уочити да се из полазног симбола F може извести било која исказна формула са словима p, p_1, p_2, ..., логичким константама $\top$ и $\bot$, и у којој се од везника појављују само негација и импликација. Изведимо, на пример формулу $\neg(p/ \Rightarrow p)$ (тј. $\neg(p_1 \Rightarrow p)$ користећи читљивији запис):

$$
\begin{array}{lll}
F & \to \neg F & [\text{применом } F \to \neg F] \\
 & \to \neg(F \Rightarrow F) & [\text{применом } F \to (F \Rightarrow F)] \\
 & \to \neg(P \Rightarrow F) & [\text{применом } F \to P] \\
 & \to \neg(P \Rightarrow P) & [\text{применом } F \to P] \\
 & \to \neg(P \Rightarrow p) & [\text{применом } P \to p] \\
 & \to \neg(P/ \Rightarrow p) & [\text{применом } P \to P/] \\
 & \to \neg(p/ \Rightarrow p) & [\text{применом } P \to p]
\end{array}
$$

Често се помоћни симболи означавају неком карактеристичном скраћеницом (или читавом речју, која се углавном наводи у посебној врсти заграда) уместо једним словом. На пример, уместо P можемо писати $\langle\texttt{slovo}\rangle$, а уместо F реч $\langle\texttt{formula}\rangle$. Уз ово означавање, правила:

$\langle\texttt{slovo}\rangle \to p, \quad \langle\texttt{slovo}\rangle \to \langle\texttt{slovo}\rangle/,$
$\langle\texttt{formula}\rangle \to \top, \quad \langle\texttt{formula}\rangle \to \bot, \quad \langle\texttt{formula}\rangle \to \langle\texttt{slovo}\rangle$
$\langle\texttt{formula}\rangle \to \neg\langle\texttt{formula}\rangle, \quad \langle\texttt{formula}\rangle \to (\langle\texttt{formula}\rangle \Rightarrow \langle\texttt{formula}\rangle)$

одсликавају индуктивну дефиницију скупа исказних формула наведеног облика.

▼ Формалне теорије

Формалну теорију чине:

- алфабет Σ;
- скуп формула $\mathrm{For} \subseteq \Sigma^*$ (који је одређен неком граматиком);
- скуп аксиома $\mathrm{Ax} \subseteq \mathrm{For}$ (из скупа свих формула издвајају се неке формуле које се сматрају аксиомама);
- скуп правила извођења $\mathcal{P}$ облика:

$$(P): \frac{\alpha_1 \quad \cdots \quad \alpha_n}{\alpha},$$

где α_1, ..., α_n, α означавају неке формуле; формуле α_1, ..., α_n називају се *премисе* (претпоставке), а формула α *закључак* правила.

Приликом задавања неке формалне теорије $\mathcal{F}$, наводимо сва четири скупа која одређују ту теорију и пишемо $\mathcal{F} = (\Sigma, \mathrm{For}, \mathrm{Ax}, \mathcal{P})$.

Дефиниција 6. *Коначан низ формула $\varphi_1, \ldots, \varphi_k$ је извођење (доказ) у формалној теорији $\mathcal{F}$ ако свака формула φ_i, $i = 1, \ldots, n$, испуњава један од услова:*

- *φ_i је аксиома, или*
- *φ_i се може добити из неких од претходних формула $\varphi_1, \ldots, \varphi_{i-1}$ применом неког од правила извођења из $\mathcal{P}$.*

Формула φ је теорема формалне теорије $\mathcal{F}$, у ознаци $\vdash_{\mathcal{F}} \varphi$ ако постоји извођење у тој теорији чији је последњи члан формула φ.

Ако је из контекста јасно о којој формалној теорији је реч, уместо $\vdash_{\mathcal{F}} \varphi$ краће пишемо $\vdash \varphi$. Уопштено говорећи, формалне теорије посматрамо као машине за производњу теорема.

Пример 19. Формална теорија $\mathcal{F}$ одређена је на следећи начин:
- алфабет садржи три симбола, $\{|, +, =\}$;
- формуле су све речи облика $x + y = z$, где су x, y, z речи записане само симболом $|$;
- једина аксиома је $| + | = ||$;
- правила извођења су:

$$(\mathrm{R1})\ \frac{x+y=z}{x|+y=z|} \qquad (\mathrm{R2})\ \frac{x+y=z}{y+x=z}$$

Докажимо $\vdash_{\mathcal{F}} ||+||| = |||||$:

1.	$\mid + \mid = \mid\mid$	аксиома
2.	$\mid\mid + \mid = \mid\mid\mid$	применом правила (R1) на формулу 1.
3.	$\mid\mid\mid + \mid = \mid\mid\mid\mid$	применом правила (R1) на формулу 2.
4.	$\mid + \mid\mid\mid = \mid\mid\mid\mid$	применом правила (R2) на формулу 3.
5.	$\mid\mid + \mid\mid\mid = \mid\mid\mid\mid\mid$	применом правила (R1) на формулу 4.

Није тешко доказати да је:

$$\vdash_{\mathcal{F}} \underbrace{|\cdots|}_{k \text{ пута}} + \underbrace{|\cdots|}_{\ell \text{ пута}} = \underbrace{|\cdots|}_{m \text{ пута}} \quad \text{акко} \quad k + \ell = m.$$

Уопштавајући концепт извођења уведен претходном дефиницијом, уводимо *извођење из хипотеза*. У наредној дефиницији подвучене су само оне речи које допуњују претходну дефиницију.

Дефиниција 7. *Нека је Γ подскуп скупа формула неке формалне теорије $\mathcal{F}$. Коначан низ формула $\varphi_1, \ldots, \varphi_k$ је извођење из хипотеза Γ у формалној теорији $\mathcal{F}$ ако свака формула φ_i, $i = 1, \ldots, n$, испуњава један од услова:*
- *φ_i је аксиома, или*
- *φ_i је хипотеза, тј. формула из Γ, или*
- *φ_i се може добити из неких од претходних формула $\varphi_1, \ldots, \varphi_{i-1}$ применом неког од правила извођења из $\mathcal{P}$.*

Формула φ је последица хипотеза Γ, у ознаци $\Gamma \vdash_{\mathcal{F}} \varphi$ ако постоји извођење из Γ чији је последњи члан формула φ.

Узимајући у обзир дефиниције 6 и 7, ознаку $\vdash_{\mathcal{F}} \varphi$ можемо схватити и као извођење формуле φ из празног скупа хипотеза.

Лема 1. *1) Ако је $\Gamma \vdash_{\mathcal{F}} \varphi$, онда $\Gamma, \theta \vdash_{\mathcal{F}} \varphi$, за било коју формулу θ. 2) Ако је $\Gamma \vdash_{\mathcal{F}} \theta$ и $\theta \vdash_{\mathcal{F}} \varphi$, онда $\Gamma \vdash_{\mathcal{F}} \varphi$.*

Лема је реч грчког порекла и означава помоћно тврђење које се користи при доказивању важних теорема.

Доказ. Тврђење 1) је очигледно. Свако извођење из скупа хипотеза Γ представља истовремено и извођење из Γ, θ. 2) Надовезивањем извођења $\Gamma \vdash_{\mathcal{F}} \theta$ и извођења $\theta \vdash_{\mathcal{F}} \varphi$, добијамо извођење $\Gamma \vdash_{\mathcal{F}} \varphi$. □

Пример 20. Нека је дата формална теорија:

- $\Sigma = \{a, b, c, d, =\}$
- формуле су речи облика $x = y$, при чему $x, y \in \{a, b, c, d\}$
- $\mathrm{Ax} = \{a = a, b = b, c = c, d = d\}$
- $\mathcal{P}$ чине два правила извођења:

$$(S): \frac{x = y}{y = x} \qquad (T): \frac{x = y \quad y = z}{x = z}.$$

Доказати $a = b, b = c, d = c \vdash a = d$.

1. $a = b$ хипотеза
2. $b = c$ хипотеза
3. $a = c$ применом правила (T) на формуле 1 и 2.
4. $d = c$ претпоставка
5. $c = d$ применом правила (S) на формулу 4.
5. $a = d$ применом правила (T) на формуле 3 и 5.

Приметимо да у извођењу није искоришћена ниједна аксиома.

Одељак завршавамо примером формалне теорије која се може препознати у многим областима математике.

Пример 21. Формалну теорију $\mathcal{O}$ одређују:

- алфабет $\Sigma = \{F, P, I, x, y, z, /, \min, \max, \leqslant\}$;
- скуп формула изграђен следећим правилима:

$P \to x \mid y \mid z \mid P/$	(у формулама се појављују променљиве, x, y, z, $x/$, $y/$, $z/$, $x//$, ..., које ћемо краће означавати $x, y, z, x_1, y_1, z_1, x_2, \ldots$)
$I \to P \mid \min(I, I) \mid \max(I, I)$	(у грађењу формула учествују изрази, изграђени од променљивих и операција min и max)
$F \to I \leqslant I$	(формуле су облика $A \leqslant B$, где су A и B неки изрази);

- аксиоме $A \leqslant A$, за било који израз A;
- правила извођења:

$$\frac{A \leqslant C}{\min(A, B) \leqslant C}\ (\min_L) \qquad \frac{A \leqslant B \quad A \leqslant C}{A \leqslant \min(B, C)}\ (\min_D)$$

$$\frac{A \leqslant C \quad B \leqslant C}{\max(A, B) \leqslant C}\ (\max_L) \qquad \frac{A \leqslant B}{A \leqslant \max(B, C)}\ (\max_D)$$

$$\frac{\min(A, B) \leqslant C}{\min(B, A) \leqslant C}\ (\min_K) \qquad \frac{A \leqslant \max(B, C)}{A \leqslant \max(C, B)}\ (\max_K)$$

$$\frac{A \leqslant B \quad B \leqslant C}{A \leqslant C}\ (T)$$

Докажимо да је $\vdash_{\mathcal{O}} \min(x, y) \leqslant \max(x, y)$.

1. $x \leqslant x$ аксиома
2. $\min(x, y) \leqslant x$ применом $(\min_L)$ на 1.
3. $\min(x, y) \leqslant \max(x, y)$ применом правила $(\max_D)$ на 2.

▼ Задаци и додаци

1. Над речима алфабета $\{A, B\}$ дозвољене су следеће трансформације: избрисати два суседна слова BB или два суседна слова AB заменити са $BBBA$; тј. $AB \to BBBA$, $BB \to$. Да ли је могуће из речи $ABBB$ добити реч:
(а) $BBBA$;
(б) $ABBBA$;
(в) $BBBBBBA$?

2. Над алфабетом $\{a, b\}$ дато је једно правило $ba \to ab$.
(а) Навести два различита извођења речи $aaabbb$ из $abbaba$.
(б) Описати све све речи из $\{a, b\}^*$ које могу бити изведене из $bbaa$.
(в) Навести скуп свих речи из $\{a, b\}^*$ из којих се може извести $aabb$.

3. MIU-систем уведен је у познатој књизи *Гедел, Ешер, Бах - једна бескарајна златна нит*:

Даглас Хофштетер је добио Пулицерову награду за ову књигу. Књига је преведена на српски.

- алфабет је $\{\mathrm{M}, \mathrm{I}, \mathrm{U}\}$;
- формуле су све речи над изабраним алфабетом;
- MI је једина аксиома;
- правила су:

(1) $\dfrac{w\mathrm{I}}{w\mathrm{IU}}$ – допиши здесна U на сваку реч која се завршава са I

(2) $\dfrac{\mathrm{M}w}{\mathrm{M}ww}$ – дуплирај реч која се надовезује на почетно M

(3) $\dfrac{v\mathrm{III}w}{v\mathrm{U}w}$ – замени III са U

(4) $\dfrac{v\mathrm{UU}w}{vw}$ – обриши UU.

Које од следећих речи су теореме овог формалног система?

(а)	MIU	(б)	MUIMUI	(в)	MIUU
(г)	MUIUIU	(д)	MIUUIIUUI	(ђ)	MIIIIIII
(е)	MIIIIII	(ж)	MIIIII	(з)	MU

4. [51] Песме класичног периода на Марсу састављене су од само две ноте, означене x и y, у складу са следећим ригорозним правилима:

[51] Specimen Test 2009, Oxford University

I Низ који не садржи ниједну ноту сматра се песмом (која се назива *тишина* и која је вероватно најпријатнија за слушање).
II Песма је и низ који започиње нотом x, затим се два пута понови иста постојећа песма и заврши се нотом y. (Другим речима, ако је W нека песма, онда је и $xWWy$ такође песма.)
III Песма је и низ нота добијен тако што се у некој постојећој песми свака нота x замени нотом y, а свака нота y нотом x.
Све песме су написане применом претходних правила.
(а) Написати четири песме дужине шест (тј. песме које су сачињене од тачно 6 нота).
(б) Колико има песама дужине 8? Колико има песама дужине 14?

(в) За које природне бројеве n постоје песме дужине n?
Упутство: Постоје песме дужине 0; ако постоје песме дужине m, онда постоје и песме дужине $2m+2$.
(г) Претпоставимо да постоји тачно k песама дужине m. Колико онда има песама дужине $2m+2$?
(д) Колико има песама дужине $2^{n+1}-2$, при чему је $n \geqslant 0$?

5. Над алфабетом $\{a,b,c\}$ дата су правила: $c \to ac$ и $c \to b$.
(а) Наћи једно извођење речи $aaab$ из речи c.
(б) Доказати да се све речи облика $a^n b$ или $a^n c$, $n \geqslant 0$, могу извести из c.
(в) Доказати да се из c могу извести само речи облика $a^n c$ или $a^n b$, $n \geqslant 0$.

6. Над алфабетом $\{a,b,S\}$ дата су правила: $S \to aSb$ и $S \to$. Доказати да се из S може извести реч w акко је w облика $a^n b^n$ или $a^n S b^n$, $n \geqslant 0$.

7. [52] Над алфабетом $\{a,b,X,Y\}$ дата су правила:

$$X \to aaYb \qquad Y \to aaYb \qquad Y \to$$

Описати скуп свих речи које се могу извести из X.

[52] Упутство. Уочити општи облик тражених речи на основу неколико конкретних извођења:

$$\begin{aligned} X &\to aaYb \\ &\to aaaaYbb \\ &\to aaaaaaYbbb \\ &\to aaaaaaaaYbbbb \\ &\to aaaaaaaabbbb \end{aligned}$$

8. Дата је формална теорија $\mathcal{F} = (\Sigma, \mathrm{For}, \mathrm{Ax}, \mathcal{P})$, при чему је:
- $\Sigma = \{a,b\}$
- $\mathrm{For} = \{a^m b a^n \mid m,n = 1,2,\ldots\}$
- $\mathrm{Ax} = \{aba, a^3ba\}$
- $\mathcal{P}$ чине три правила извођења:

$$(A): \frac{a^m b a^n}{a^n b a^m} \qquad (B): \frac{a^m b a^n}{a^{m+1} b a^{n+1}} \qquad (C): \frac{a^k b a^m \quad a^m b a^n}{a^k b a^n}.$$

(а) Навести једно извођење формуле $a^5 ba$.
(б) Ако је $m+n$ паран број, доказати да је $\vdash_{\mathcal{F}} a^m b a^n$;
(в) Ако је $\vdash_{\mathcal{F}} a^m b a^n$, доказати да је $m+n$ паран број.

9. Формална теорија $\mathcal{M}$ одређена је на следећи начин:
- алфабет: $\{\leftrightarrow, \mathtt{t}, \mathtt{n}\}$;
- формуле су све речи облика $\alpha \leftrightarrow \beta$, где су α, β речи записане само симболима $\mathtt{t}$, $\mathtt{n}$;
- аксиоме су $\mathtt{n} \leftrightarrow \mathtt{n}$, $\mathtt{t} \leftrightarrow \mathtt{t}$, $\mathtt{nn} \leftrightarrow \mathtt{n}$, $\mathtt{nt} \leftrightarrow \mathtt{n}$, $\mathtt{tn} \leftrightarrow \mathtt{n}$, $\mathtt{tt} \leftrightarrow \mathtt{t}$;
- правила извођења су:

$$(\mathrm{T})\ \frac{\alpha \leftrightarrow \beta \quad \beta \leftrightarrow \gamma}{\alpha \leftrightarrow \gamma} \qquad (\mathrm{S})\ \frac{\alpha \leftrightarrow \beta}{\beta \leftrightarrow \alpha} \qquad (\mathrm{K})\ \frac{\alpha \leftrightarrow \beta \quad \gamma \leftrightarrow \delta}{\alpha\gamma \leftrightarrow \beta\delta}$$

Доказати $\vdash_{\mathcal{M}} \mathtt{tnn} \leftrightarrow \mathtt{ntt}$.

10. Формална теорија $\mathcal{F}$ је одређена на следећи начин:
- алфабет садржи три симбола, $\{|, *, =\}$;
- формуле су све речи облика $x * y = z$, где су x, y, z речи записане само симболом $|$;
- једина аксиома је формула $|| * | = |$;
- правила извођења су:

$$(\mathrm{R1})\ \frac{x * y = z}{x| * y = z|} \qquad (\mathrm{R2})\ \frac{x * y = z|}{x * y| = z}$$

(а) Доказати $\vdash_{\mathcal{F}} ||||| * ||| = ||$.

(б) Ако је $\vdash_{\mathcal{F}} \underbrace{||\cdots|}_{73\text{ пута}} * \underbrace{||\cdots|}_{37\text{ пута}} = \underbrace{||\cdots|}_{k\text{ пута}}$, одредити k.

11. Формална теорија $\mathcal{F}$ је одређена на следећи начин:

• алфабет садржи три симбола, $\{|, *, =\}$;

• формуле су све речи облика $x * y = z$, где су x, y, z речи записане само симболом $|$;

• једина аксиома је формула $| * | = |$;

• правила извођења су:

$$(\text{R1})\ \frac{x * y = z}{x * y| = zx} \qquad (\text{R2})\ \frac{x * y = z}{y * x = z}$$

(а) Доказати $\vdash_{\mathcal{F}} ||| * || = ||||||$.

(б) Ако је $\vdash_{\mathcal{F}} \underbrace{||\cdots|}_{20\text{ пута}} * \underbrace{||\cdots|}_{22\text{ пута}} = \underbrace{||\cdots|}_{k\text{ пута}}$, одредити k.

12. Нека је дата формална теорија:

• $\Sigma = \{a, b, c, d, =\}$

• формуле су речи облика $x = y$, при чему $x, y \in \{a, b, c, d\}$

• $\text{Ax} = \emptyset$

• $\mathcal{P}$ чине два правила извођења:

$$(S):\ \frac{x = y}{y = x} \qquad (T):\ \frac{x = y \quad y = z}{x = z}.$$

Доказати:

(а) $a = b, b = c, c = d \vdash d = a$

(б) $a = d, c = d \vdash c = a$

(в) $b = a, c = a \vdash a = a$

13. [53] Над алфабетом $\Sigma = \{F, P, I, x, y, z, /, \min, \max, \leqslant\}$, скуп формула је изграђен следећим правилима:

• $P \to x \mid y \mid z \mid P/$ (у формулама се појављују променљиве, x, y, z, $x/$, $y/$, $z/$, $x//$, $y//$, $z//$, $\dots$, које ћемо краће означавати $x, y, z, x_1, y_1, z_1, x_2, y_2, z_2, \dots$)

• $I \to P \mid \min(I, I) \mid \max(I, I)$ (у грађењу формула учествују изрази, изграђени од променљивих и операција min и max)

• $F \to I \leqslant I$ (формуле су облика $A \leqslant B$, где су A и B неки изрази.) Аксиоме су формуле облика $A \leqslant A$, за било који израз A. Правила извођења су:

$$\frac{A \leqslant C}{\min(A, B) \leqslant C}\ (\min_L) \qquad \frac{A \leqslant B \quad A \leqslant C}{A \leqslant \min(B, C)}\ (\min_D)$$

$$\frac{A \leqslant C \quad B \leqslant C}{\max(A, B) \leqslant C}\ (\max_L) \qquad \frac{A \leqslant B}{A \leqslant \max(B, C)}\ (\max_D)$$

$$\frac{\min(A, B) \leqslant C}{\min(B, A) \leqslant C}\ (\min_K) \qquad \frac{A \leqslant \max(B, C)}{A \leqslant \max(C, B)}\ (\max_K)$$

$$\frac{A \leqslant B \quad B \leqslant C}{A \leqslant C}\ (T)$$

[53] Ова формална теорија је уведена и у примеру 21, на страни 42.

Доказати:
(а) $\vdash x \leqslant \min(x, \max(x,y))$
(б) $\vdash \max(x, \min(x,y)) \leqslant x$
(в) $\vdash \max(x, \min(y,z)) \leqslant \min(\max(x,y), \max(x,z))$
(г) $\vdash \min(x, \max(y,z)) \leqslant \max(\min(x,y), \min(x,z))$

14. Алфабет и формуле формалне теорије су одређене правилима:

• $P \to x \mid y \mid z \mid P/$ (у формулама се појављују променљиве, x, y, z, $x/$, $y/$, $z/$, $x//$, $y//$, $z//$, …, које ћемо краће означавати $x, y, z, x_1, y_1, z_1, x_2, y_2, z_2, \dots$)

• $I \to P \mid (I * I)$ (у грађењу формула учествују изрази, изграђени од променљивих и операције $*$)

• $F \to I = I$ (формуле су облика $A = B$, где су A и B неки изрази.)

Аксиоме су формуле облика $A * (B * C) = (A * B) * C$, за било које изразе A, B, C.

Правила извођења су:

$$\frac{}{A = A}\,(=_R) \qquad \frac{A = B}{B = A}\,(=_S)$$

$$\frac{A = B \quad B = C}{A = C}\,(=_D) \qquad \frac{A = B \quad C = D}{(A * C) = (B * D)}\,(=_D)$$

Доказати: $\vdash ((x * y) * (x_1 * z)) = (x * ((y * x_1) * z))$.

15. Алфабет и формуле су одређене правилима:

• $P \to x \mid y \mid z \mid P/$ (у формулама се појављују променљиве, x, y, z, $x/$, $y/$, $z/$, $x//$, $y//$, $z//$, …, које ћемо краће означавати $x, y, z, x_1, y_1, z_1, x_2, y_2, z_2, \dots$)

• $I \to P \mid \mathbf{e} \mid I^- \mid (I * I)$

• $F \to I = I$ (формуле су облика $A = B$, где су A и B неки изрази.)

Аксиоме су формуле облика:[54]

• $A * (B * C) = (A * B) * C$, за било које изразе A, B, C,

• $A * \mathbf{e} = A$ и $\mathbf{e} * A = A$, за било који израз A,

• $A * A^- = \mathbf{e}$ и $A^- * A = \mathbf{e}$, за било који израз A;

Правила извођења су:

$$\frac{}{A = A}\,(=_R) \qquad \frac{A = B}{B = A}\,(=_S)$$

$$\frac{A = B \quad B = C}{A = C}\,(=_D) \qquad \frac{A = B \quad C = D}{(A * C) = (B * D)}\,(=_D)$$

Доказати: $\vdash x^{--} = x$.

16. Формални систем је одређен на следећи начин:

• $\Sigma = \{a, b, c, d, \prec, \not\prec, \perp\}$

• формуле су $\perp$ и све речи облика $x \prec y$ или $x \not\prec y$, при чему $x, y \in \{a, b, c, d\}$

• $\mathrm{Ax} = \emptyset$

[54] Изостављамо неке заграде да бисмо поједноставили запис.

- правила извођења су:

$$(I):\ \frac{x \prec x}{\bot} \qquad (T):\ \frac{x \prec y \quad y \prec z}{x \prec z} \qquad (C):\ \frac{x \prec y \quad x \not\prec y}{\bot}$$

и следеће (RAA)-правило Reductio Ad Absurdum:

(RAA) Ако се $\bot$ може извести из полазних претпоставки и **додатне претпоставке** облика $x \prec y$ (односно $x \not\prec y$), онда се **без** те додатне претпоставке може извести $x \not\prec y$ (односно $x \prec y$).

Правило (RAA) кратко записујемо на следећи начин:

$$\begin{array}{|c} x \prec y \\ \vdots \\ \bot \\ \hline \end{array} \quad \frac{}{x \not\prec y}\ (RAA) \qquad \begin{array}{|c} x \not\prec y \\ \vdots \\ \bot \\ \hline \end{array} \quad \frac{}{x \prec y}\ (RAA)$$

Доказати:

(а) $a \prec b, b \prec c, c \prec a \vdash \bot$

(б) $a \prec b, b \prec c \vdash c \not\prec a$

1.3 Исказни рачун Ł (Формална теорија Ł)

Увод. Свака исказна формула, са n исказних слова, одређује један n-арни везник, тј. функцију која свакој од 2^n валуација додељује одговарајућу истинитосну вредност формуле. Сваки n-арни везник потпуно је одређен истинитосном таблицом и једноставно се може описати формулом у којој се појављују само везници $\neg, \wedge, \vee$ (подсећамо да је свака исказна формула еквивалентна некој формули у конјунктивној, одн. дисјунктивној нормалној форми). Због чињенице да се сваки логички везник може изразити везницима $\neg, \wedge, \vee$, кажемо да је $\{\neg, \wedge, \vee\}$ *потпун систем везника.*

Познато је како се помоћу $\neg, \wedge, \vee$ уводе логичке константе и остали исказни везници: $\perp$ уводимо као скраћење за $p \wedge \neg p$, где је p неко исказно слово, $\top$ као скраћење за $\neg\perp$, $\alpha \Rightarrow \beta$ као скраћење за $\neg\alpha \vee \beta$, и $\alpha \Leftrightarrow \beta$ као скраћење за $(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$, односно $(\neg\alpha \vee \beta) \wedge (\neg\beta \vee \alpha)$.

Негација и импликација, $\{\neg, \Rightarrow\}$ такође чине један потпун систем везника. Према претходном, довољно је изразити конјункцију и дисјункцију:

$\alpha \vee \beta \equiv \neg\alpha \Rightarrow \beta$,

$\alpha \wedge \beta \equiv \neg(\alpha \Rightarrow \neg\beta)$.

Приметимо и да је:

$\top \equiv (p \Rightarrow p)$, за било које слово p,

$\perp \equiv \neg\top \equiv \neg(p \Rightarrow p)$,

$\alpha \Leftrightarrow \beta \equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha) \equiv \neg((\alpha \Rightarrow \beta) \Rightarrow \neg(\beta \Rightarrow \alpha))$.

Наведене еквиваленције можемо схватити и као правила за трансформацију било које исказне формуле у еквивалентан облик у коме се појављују само везници $\neg$ и $\Rightarrow$. На пример,

$$\begin{aligned}(\neg p \wedge q) \Leftrightarrow (p \vee q) &\equiv \neg(\neg p \Rightarrow \neg q) \Leftrightarrow (\neg p \Rightarrow q)\\ &\equiv (\neg(\neg p \Rightarrow \neg q) \Rightarrow (\neg p \Rightarrow q)) \wedge ((\neg p \Rightarrow q) \Rightarrow \neg(\neg p \Rightarrow \neg q))\\ &\equiv \neg((\neg(\neg p \Rightarrow \neg q) \Rightarrow (\neg p \Rightarrow q)) \Rightarrow \neg((\neg p \Rightarrow q) \Rightarrow \neg(\neg p \Rightarrow \neg q)))\end{aligned}$$

Овај потпуни систем везника искористићемо да уведемо једну формалну теорију која ће бити 'машина за производњу' таутологија.

Постоји и једночлани потпуни системи везника. Пример таквог везника је Лукасиевичева стрелица $\downarrow$ дата таблицом:

$\downarrow$	0	1
0	1	0
1	0	0

Овај везник читамо *нили* (ни $\cdots$ ни $\cdots$). Није тешко уочити да је:

$\neg\alpha \equiv \alpha \downarrow \alpha$,

$\alpha \Rightarrow \beta \equiv \neg(\neg\alpha \downarrow \beta)$

$\equiv ((\alpha \downarrow \alpha) \downarrow \beta) \downarrow ((\alpha \downarrow \alpha) \downarrow \beta)$.

План

- исказни рачун Ł: алфабет, формуле, аксиоме, правила извођења
- теорема сагласности
- теорема дедукције
- теорема потпуности

Посебно издвајамо формалну теорију познату као (Лукасиевичев) исказни рачун Ł:

Јан Лукасиевич (1878–1956), пољски математичар

Прецизније, алфабет и формуле су одређене правилима:
$P \to p \mid q \mid r \mid P/$
$F \to P \mid \neg F \mid (F \Rightarrow F)$
Наравно, примењујемо и стандардне договоре о брисању заграда.

- алфабет чине логички везници $\Rightarrow$, $\neg$, заграде (,) и исказна слова $p, q, r, \ldots, p_n, q_n, r_n, \ldots$;
- формуле су све исказне формуле изграђене на уобичајен начин (у којима се појављују само симболи уведеног афабета);
- аксиоме су следећег облика:
  - A1 $\alpha \Rightarrow (\beta \Rightarrow \alpha)$
  - A2 $(\alpha \Rightarrow (\beta \Rightarrow \gamma)) \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow (\alpha \Rightarrow \gamma))$
  - A3 $(\neg\beta \Rightarrow \neg\alpha) \Rightarrow (\alpha \Rightarrow \beta)$

  где су α, β, γ произвољне формуле;
- једино правило извођења је модус поненс:
  $$\frac{\alpha \qquad \alpha \Rightarrow \beta}{\beta}\ (MP)$$
  где су α, β произвољне формуле.

Лема 2. *$\vdash_{Ł} \alpha \Rightarrow \alpha$, за било коју формулу α.*

Доказ.

1.	$(\alpha \Rightarrow ((\alpha \Rightarrow \alpha) \Rightarrow \alpha)) \Rightarrow ((\alpha \Rightarrow (\alpha \Rightarrow \alpha)) \Rightarrow (\alpha \Rightarrow \alpha))$	аксиома A2
2.	$\alpha \Rightarrow ((\alpha \Rightarrow \alpha) \Rightarrow \alpha)$	аксиома A1
3.	$(\alpha \Rightarrow (\alpha \Rightarrow \alpha)) \Rightarrow (\alpha \Rightarrow \alpha)$	$MP(2,1)$
4.	$\alpha \Rightarrow (\alpha \Rightarrow \alpha)$	аксиома A1
5.	$\alpha \Rightarrow \alpha$	$MP(4,3)$

Наведени низ формула представља извођење формуле $\alpha \Rightarrow \alpha$ у рачуну Ł. □

Лема 3. *За произвољне формуле α, β, γ:*
(i) $\alpha \Rightarrow \beta, \beta \Rightarrow \gamma, \alpha \vdash_{Ł} \gamma$
(ii) $\alpha, \neg\alpha \vdash_{Ł} \beta$

Доказ. (i) Треба пронаћи извођење формуле γ користећи хипотезе $\alpha \Rightarrow \beta, \beta \Rightarrow \gamma, \alpha$:

1.	$\alpha \Rightarrow \beta$	хипотеза
2.	α	хипотеза
3.	β	$MP(2,1)$
4.	$\beta \Rightarrow \gamma$	хипотеза
5.	γ	$MP(3,4)$

(ii) Доказујемо да „из противречних тврдњи можемо извести било који закључак”:

1.	α	хипотеза
2.	$\neg\alpha$	хипотеза
3.	$\neg\alpha \Rightarrow (\neg\beta \Rightarrow \neg\alpha)$	A1
4.	$\neg\beta \Rightarrow \neg\alpha$	$MP(2,3)$
5.	$(\neg\beta \Rightarrow \neg\alpha) \Rightarrow (\alpha \Rightarrow \beta)$	A3
6.	$\alpha \Rightarrow \beta$	$MP(4,5)$
7.	β	$MP(1,6)$ □

Природно се намеће проблем: *описати све теореме рачуна* Ł. Испоставља се да је исказна формула φ (над алфабетом рачуна Ł) теорема, тј. $\vdash_Ł \varphi$ акко је φ таутологија.

Подсећамо да је $\{\Rightarrow, \neg\}$ је потпун систем везника, и да се исказни везници $\vee$, $\wedge$, $\Leftrightarrow$ могу изразити помоћу $\Rightarrow$ и $\neg$:

$$\begin{aligned} \alpha \vee \beta &\equiv \neg\alpha \Rightarrow \beta \\ \alpha \wedge \beta &\equiv \neg\alpha \vee \neg\beta \\ \alpha \Leftrightarrow \beta &\equiv (\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha) \end{aligned}$$

Теорема 7. [***Теорема сагласности***] *Ако је* $\vdash_Ł \varphi$, *онда је* φ *таутологија.*

ДОКАЗ. Довољно је доказати:

- Аксиоме A1, A2 и A3 јесу таутологије;
- Правило извођења (MP) *чува* таутологије, тј. ако су α и $\alpha \Rightarrow \beta$ таутологије, онда је и β таутологија.

Показаћемо само ово друго. Ако су α и $\alpha \Rightarrow \beta$ таутологије, не може постојати валуација за коју би формула β била нетачна. Уколико би за неку валуацију формула β била нетачна, за ту валуацију би α било тачно (јер је α таутологија), па би импликација $\alpha \Rightarrow \beta$ била нетачна, што је немогуће, јер је $\alpha \Rightarrow \beta$ таутологија. □

Важи и обрат претходне теореме: у формалној теорији Ł могу се извести само таутологије. Прво доказујемо следећу важну теорему.

Теорема 8. [***Теорема дедукције***] *Ако је* Γ *неки скуп формула и нека су* α, β *произвољне формуле.*

$$\Gamma, \alpha \vdash_Ł \beta \text{ акко } \Gamma \vdash_Ł \alpha \Rightarrow \beta$$

ДОКАЗ. $(\leftarrow)$ Доказујемо прво једноставнији део, да из $\Gamma \vdash_Ł \alpha \Rightarrow \beta$ следи $\Gamma, \alpha \vdash_Ł \beta$.

Претпоставимо да $\Gamma \vdash_Ł \alpha \Rightarrow \beta$. Нека је $\varphi_1, \ldots, \varphi_m$ извођење формуле $\alpha \Rightarrow \beta$ из Γ (при чему је, наравно, φ_m формула $\alpha \Rightarrow \beta$). Тада је следећи низ формула извођење формуле β из Γ, α:

1.	φ_1	
	$\vdots$	
m.	$\alpha \Rightarrow \beta$	
$(m+1)$.	α	хипотеза
$(m+2)$.	β	$MP(m+1, m)$

$(\rightarrow)$ Претпоставимо $\Gamma, \alpha \vdash_Ł \beta$. Треба да докажемо да $\Gamma \vdash_Ł \alpha \Rightarrow \beta$.

Водећа замисао у доказу овог дела теореме јесте како извођење $\Gamma, \alpha \vdash_Ł \beta$ **прерадити** у извођење $\Gamma \vdash_Ł \alpha \Rightarrow \beta$. Ту прераду одређујемо индукцијом по дужини извођења $\Gamma, \alpha \vdash_Ł \beta$.

Доказ спроводимо индукцијом по дужини извођења формуле β из хипотеза Γ, α.

(БИ) Претпоставимо да се извођења формуле β из хипотеза Γ, α састоји из само једне формуле. Тада та једина формула у извођењу мора бити управо формула β. Самим тим β је аксиома или је β хипотеза, тј. $\beta \in \Gamma$ или је β истоветна формули α. Дакле, могућ је један од следећа три случаја:

- β **је аксиома** – тада је следећи низ формула извођење формуле $\alpha \Rightarrow \beta$ из Γ:

Битно све

1.	β	аксиома
2.	$\beta \Rightarrow (\alpha \Rightarrow \beta)$	аксиома А1
3.	$\alpha \Rightarrow \beta$	$MP(1,2)$

- β **припада** Γ – слично као у претходном случају добијамо извођење формуле $\alpha \Rightarrow \beta$ из Γ:

1.	β	хипотеза
2.	$\beta \Rightarrow (\alpha \Rightarrow \beta)$	аксиома А1
3.	$\alpha \Rightarrow \beta$	$MP(1,2)$

- β **је заправо формула** α – онда, према леми 2 $\vdash_{Ł} \alpha \Rightarrow \alpha$, а самим тим и $\Gamma \vdash_{Ł} \alpha \Rightarrow \alpha$.

База индукције је доказана.

(ИП) Претпоставимо да за свако $k < n$, ако постоји извођење дужине k формуле β из претпоставки Γ, α, онда постоји извођење формуле $\alpha \Rightarrow \beta$ из Γ.

Нека је $\varphi_1, \ldots, \varphi_n$ извођење дужине n формуле β из Γ, α; дакле φ_n је формула β. Тада, према дефиницији 7 (страна 41) наступа један од следећих случајева: (1°) β је аксиома, или (2°) β припада Γ, или (3°) β је формула α, или

(4°) β је добијена применом (MP) на неке формуле φ_i и φ_j, за неке $i, j < n$, при чему је формула φ_j заправо $\varphi_i \Rightarrow \beta$.

У случајевима (1°), (2°), (3°) закључујемо као у бази индукције. Преостаје да размотримо случај (4°). Тада извођење има следећи облик:

1.	φ_1	
	$\vdots$	
i.	φ_i	
	$\vdots$	
j.	$\varphi_i \Rightarrow \beta$	
	$\vdots$	
n.	β	$MP(i,j)$

Првих i формула представљају извођење формуле φ_i из Γ, α. Према индуктивној хипотези, јер је $i < n$, постоји извођење формуле $\alpha \Rightarrow \varphi_i$ из Γ:

$\psi_1, \ldots, \psi_\ell$, при чему је ψ_ℓ формула $\alpha \Rightarrow \varphi_i$.

Такође, првих j формула чине извођење за $\varphi_i \Rightarrow \beta$ из Γ, α. Поново према индуктивној хипотези, јер је $j < n$, постоји извођење формуле $\alpha \Rightarrow (\varphi_i \Rightarrow \beta)$ из Γ:

$\theta_1, \ldots, \theta_k$, при чему је θ_k формула $\alpha \Rightarrow (\varphi_i \Rightarrow \beta)$.

Надовезивањем ова два извођења и додавањем још три корака добијамо извођење формуле $\alpha \Rightarrow \beta$ из Γ:

1.	ψ_1	
	$\vdots$	
ℓ.	$\alpha \Rightarrow \varphi_i$	
$(\ell+1)$.	θ_1	
	$\vdots$	
$(\ell+k)$.	$\alpha \Rightarrow (\varphi_i \Rightarrow \beta)$	
$(\ell+k+1)$.	$(\alpha \Rightarrow (\varphi_i \Rightarrow \beta)) \Rightarrow ((\alpha \Rightarrow \varphi_i) \Rightarrow (\alpha \Rightarrow \beta))$	аксиома А2
$(\ell+k+2)$.	$(\alpha \Rightarrow \varphi_i) \Rightarrow (\alpha \Rightarrow \beta)$	$MP(\ell+k, \ell+k+1)$
$(\ell+k+3)$.	$\alpha \Rightarrow \beta$	$MP(\ell, \ell+k+2)$

Дакле, за свако извођење формуле β из Γ, α, постоји извођење формуле $\alpha \Rightarrow \beta$ из Γ. □

Применом теореме дедукције, из

$$\alpha \Rightarrow \beta, \beta \Rightarrow \gamma, \alpha \vdash_{Ł} \gamma \text{ (лема 3 (i))}$$

добијамо, на пример:

- $\alpha \Rightarrow \beta, \beta \Rightarrow \gamma \vdash_{Ł} \alpha \Rightarrow \gamma$
- $\alpha \Rightarrow \beta, \alpha \vdash_{Ł} (\beta \Rightarrow \gamma) \Rightarrow \gamma$
- $\alpha \Rightarrow \beta \vdash_{Ł} (\beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma)$
- $\vdash_{Ł} (\alpha \Rightarrow \beta) \Rightarrow ((\beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma))$ итд.

Штавише, једноставно се уочава да у извођењима можемо користити следеће изведено правило:

$$\frac{\alpha \Rightarrow \beta \quad \beta \Rightarrow \gamma}{\alpha \Rightarrow \gamma} \; (T)$$

које обележамо (T) и називамо *транзитивност импликације*.

Такође, из

$$\alpha, \neg\alpha \vdash_{Ł} \beta \text{ (лема 3 (ii))}$$

добијамо, на пример:

- $\alpha \vdash_{Ł} \neg\alpha \Rightarrow \beta$
- $\vdash_{Ł} \alpha \Rightarrow (\neg\alpha \Rightarrow \beta)$
- $\vdash_{Ł} \neg\alpha \Rightarrow (\alpha \Rightarrow \beta)$ итд.

Лема 4. *За произвољне формуле α, β:*

Користити теорему дедукције када год је то погодно.

(i) $\vdash_{Ł} \neg\neg\alpha \Rightarrow \alpha$
(ii) $\vdash_{Ł} \alpha \Rightarrow \neg\neg\alpha$
(iii) $\vdash_{Ł} (\alpha \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \neg\alpha)$
(iv) $\alpha \Rightarrow \beta, \neg\alpha \Rightarrow \beta \vdash_{Ł} \beta$

Доказ.
(i) Применом теореме дедукције, довољно је доказати $\neg\neg\alpha \vdash_{Ł} \alpha$

1.	$\neg\neg\alpha$	хипотеза
2.	$\neg\neg\alpha \Rightarrow (\neg\alpha \Rightarrow \neg\neg\neg\alpha)$	последица леме 3 (ii) и теореме дедукције
3.	$\neg\alpha \Rightarrow \neg\neg\neg\alpha$	$MP(1, 2)$
4.	$(\neg\alpha \Rightarrow \neg\neg\neg\alpha) \Rightarrow (\neg\neg\alpha \Rightarrow \alpha)$	А3
5.	$\neg\neg\alpha \Rightarrow \alpha$	$MP(3, 4)$
6.	α	$MP(1, 5)$

битно

(ii)

1.	$\neg\neg\neg\alpha \Rightarrow \neg\alpha$	према (i)
2.	$(\neg\neg\neg\alpha \Rightarrow \neg\alpha) \Rightarrow (\alpha \Rightarrow \neg\neg\alpha)$	A3
3.	$\alpha \Rightarrow \neg\neg\alpha$	$MP(1,2)$

(iii) Доказујемо $\alpha \Rightarrow \beta \vdash_{Ł} \neg\beta \Rightarrow \neg\alpha$

1.	$\alpha \Rightarrow \beta$	хипотеза
2.	$(\neg\neg\alpha \Rightarrow \neg\neg\beta) \Rightarrow (\neg\beta \Rightarrow \neg\alpha)$	A3
3.	$\neg\neg\alpha \Rightarrow \alpha$	према (i)
4.	$\neg\neg\alpha \Rightarrow \beta$	$T(3,1)$
5.	$\beta \Rightarrow \neg\neg\beta$	према (ii)
6.	$\neg\neg\alpha \Rightarrow \neg\neg\beta$	$T(4,5)$
7.	$\neg\beta \Rightarrow \neg\alpha$	$MP(6,2)$

(iv) Доказујемо $\alpha \Rightarrow \beta, \neg\alpha \Rightarrow \beta \vdash_{Ł} \beta$

1.	$\alpha \Rightarrow \beta$	хипотеза
2.	$\neg\alpha \Rightarrow \beta$	хипотеза
3.	$\neg\beta \Rightarrow \neg\alpha$	(iii)
4.	$\neg\beta \Rightarrow \beta$	$T(3,2)$
5.	$\neg\beta \Rightarrow (\beta \Rightarrow \neg(\beta \Rightarrow \beta))$	Лема 3 (ii) и теорема дедукције (два пута)
6.	$\neg\beta \Rightarrow (\beta \Rightarrow \neg(\beta \Rightarrow \beta)) \Rightarrow ((\neg\beta \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \neg(\beta \Rightarrow \beta)))$	A2
7.	$(\neg\beta \Rightarrow \beta) \Rightarrow (\neg\beta \Rightarrow \neg(\beta \Rightarrow \beta))$	$MP(5,6)$
8.	$\neg\beta \Rightarrow \neg(\beta \Rightarrow \beta)$	$MP(4,7)$
9.	$(\neg\beta \Rightarrow \neg(\beta \Rightarrow \beta)) \Rightarrow ((\beta \Rightarrow \beta) \Rightarrow \beta)$	A3
10.	$(\beta \Rightarrow \beta) \Rightarrow \beta$	$MP(8,9)$
11.	$\beta \Rightarrow \beta$	Лема 2
12.	β	$MP(11,10)$ □

Претходна лема (iii) и (iv) оправдава и употребу следећих изведених правила:

$$\frac{\alpha \Rightarrow \beta}{\neg\beta \Rightarrow \neg\alpha}\ (K) \qquad \frac{\alpha \Rightarrow \beta \quad \neg\alpha \Rightarrow \beta}{\beta}\ (C)$$

У доказу најављеног тврђења:

$$\text{ако } \models \varphi, \text{ онда } \vdash_{Ł} \varphi$$

кључну улогу има запажање да се у рачуну Ł може (у извесном смислу) *извести* истинитосна таблица импликације. Наредном лемом се прецизира ово запажање.

Лема 5. [62] *За произвољне формуле* α, β:

(i) $\alpha, \beta \vdash_{Ł} \alpha \Rightarrow \beta$

(ii) $\alpha, \neg\beta \vdash_{Ł} \neg(\alpha \Rightarrow \beta)$

(iii) $\neg\alpha, \beta \vdash_{Ł} \alpha \Rightarrow \beta$

(iv) $\neg\alpha, \neg\beta \vdash_{Ł} \alpha \Rightarrow \beta$

[62] Упоредити тврђења леме и таблицу:

α	β	$\alpha \Rightarrow \beta$
1	1	1
1	0	0
0	1	1
0	0	1

ДОКАЗ.

(i)

1.	β	хипотеза
2.	$\beta \Rightarrow (\alpha \Rightarrow \beta)$	A1
3.	$\alpha \Rightarrow \beta$	$MP(1,2)$

битно

(ii)

1.	α	хипотеза
2.	$\neg\beta$	хипотеза
3.	$\alpha \Rightarrow ((\alpha \Rightarrow \beta) \Rightarrow \beta)$	из $\alpha, \alpha \Rightarrow \beta \vdash_{Ł} \beta$, према теореми дедукције
4.	$(\alpha \Rightarrow \beta) \Rightarrow \beta$	$MP(1,3)$
5.	$\neg\beta \Rightarrow \neg(\alpha \Rightarrow \beta)$	$K(4)$
6.	$\neg(\alpha \Rightarrow \beta)$	$MP(2,5)$

(iii)-(iv) Према леми 3 (ii) и теореми дедукције важи $\neg\alpha \vdash_{Ł} \alpha \Rightarrow \beta$, па самим тим важи и $\neg\alpha, \beta \vdash_{Ł} \alpha \Rightarrow \beta$ и $\neg\alpha, \neg\beta \vdash_{Ł} \alpha \Rightarrow \beta$. □

Запажања из претходне леме можемо другачије формулисати, користећи једну нову ознаку. Ако је v нека валуација исказних слова и φ произвољна формула, нека је $v(\varphi)$ истинитосна вредност формуле φ при валуацији v и

$$\varphi^v = \begin{cases} \varphi, & \text{ако је } v(\varphi) = 1, \\ \neg\varphi, & \text{ако је } v(\varphi) = 0. \end{cases}$$

Уз ове ознаке, тврђења (i)-(iv) претходне леме обједињено исказујемо следећом последицом.

Последица 1. Ако је v валуација и α, β произвољне исказне формуле, онда $\alpha^v, \beta^v \vdash_{Ł} (\alpha \Rightarrow \beta)^v$.

Последицу можемо неформално разумети на следећи начин: ако знамо истинитосне вредности формула α и β, онда у Ł можемо „израчунати" истинитисну вредност формуле $\alpha \Rightarrow \beta$.
Ако знамо истинитосну вредност формуле α, онда у Ł можемо „израчунати" истинитисну вредност формуле $\neg\alpha$.

Слично тврђење важи и за негацију.

Последица 2. Ако је v валуација и α произвољна исказна формула, онда $\alpha^v \vdash_{Ł} (\neg\alpha)^v$.

Доказ. Разликујемо два случаја.

1. случај: $v(\alpha) = 0$. Тада је α^v формула $\neg\alpha$, и $v(\neg\alpha) = 1$, па је $(\neg\alpha)^v$ такође формула $\neg\alpha$. Очигледно, $\neg\alpha \vdash_{Ł} \neg\alpha$, тј. $\alpha^v \vdash_{Ł} (\neg\alpha)^v$ и тврђење је доказано.

2. случај: $v(\alpha) = 1$. Тада је α^v формула α, и $v(\neg\alpha) = 0$, па је $(\neg\alpha)^v$ формула $\neg\neg\alpha$. Из $\alpha \vdash_{Ł} \neg\neg\alpha$ следи да и у овом случају важи $\alpha^v \vdash_{Ł} (\neg\alpha)^v$. □

Претходне две последице обједињујемо у једно важно запажање.

Последица 3. Нека је φ нека формула у којој се појављују само (не нужно сва) слова $p_1, \dots, p_k$. Тада за сваку валуацију v важи: $p_1^v, \dots, p_k^v \vdash_{Ł} \varphi^v$.

Доказ. Индукцијом по сложености формуле.

(БИ) Тврђење очигледно важи ако је φ исказно слово.

(ИП) Претпоставимо да тврђење важи за све формуле које су мање сложености од φ.

Нека је φ облика $\neg\alpha$. Према (ИП): $p_1^v, \dots, p_k^v \vdash_{Ł} \alpha^v$. Према Последици 2, $\alpha^v \vdash_{Ł} (\neg\alpha)^v$, одакле следи $p_1^v, \dots, p_k^v \vdash_{Ł} (\neg\alpha)^v$, тј. $p_1^v, \dots, p_k^v \vdash_{Ł} \varphi^v$.

Нека је φ облика $\alpha \Rightarrow \beta$. Према индуктивној претпоставци је $p_1^v, \dots, p_k^v \vdash_{Ł} \alpha^v$ и $p_1^v, \dots, p_k^v \vdash_{Ł} \beta^v$. Када применимо Последицу 1, $\alpha^v, \beta^v \vdash_{Ł} (\alpha \Rightarrow \beta)^v$, добијамо $p_1^v, \dots, p_k^v \vdash_{Ł} (\alpha \Rightarrow \beta)^v$, тј. $p_1^v, \dots, p_k^v \vdash_{Ł} \varphi^v$. □

битно

Пример 22. За формулу $((r \Rightarrow \neg s) \Rightarrow p) \Rightarrow \neg q$ је приказан део истинитосне таблице:

p	q	r	s	$\cdots$	$((r \Rightarrow \neg s) \Rightarrow p) \Rightarrow \neg q$
0	1	1	1	$\cdots$	0
1	0	0	1	$\cdots$	1
1	1	1	1	$\cdots$	0

Према последици 3, закључујемо:
- $\neg p, q, r, s \vdash_Ł \neg(((r \Rightarrow \neg s) \Rightarrow p) \Rightarrow \neg q)$
- $p, \neg q, \neg r, s \vdash_Ł ((r \Rightarrow \neg s) \Rightarrow p) \Rightarrow \neg q$
- $p, q, r, s \vdash_Ł \neg(((r \Rightarrow \neg s) \Rightarrow p) \Rightarrow \neg q)$

Теорема 9. [**Теорема потпуности**] *Ако је φ таутологија, онда $\vdash_Ł \varphi$.*

Доказ. Нека су $p_1, \ldots, p_k$ слова која се појављују у φ. За било коју валуацију v слова $p_1, \ldots, p_k$ важи $\varphi^v = \varphi$, као и (последица 2) $p_1^v, \ldots, p_k^v \vdash \varphi$.

Нека је w произвољна валуација. Тада

$$p_1^w, \ldots, p_{k-1}^w, p_k \vdash \varphi \text{ и } p_1^w, \ldots, p_{k-1}^w, \neg p_k \vdash \varphi,$$

односно

$$p_1^w, \ldots, p_{k-1}^w \vdash p_k \Rightarrow \varphi \text{ и } p_1^w, \ldots, p_{k-1}^w \vdash \neg p_k \Rightarrow \varphi,$$

Лема 4 (iv) оправдава употребу правила

$$\frac{\alpha \Rightarrow \beta \quad \neg\alpha \Rightarrow \beta}{\beta}\ (C)$$

одакле следи $p_1^w, \ldots, p_{k-1}^w \vdash \varphi$. Настављајући овај поступак, добијамо $p_1^w, \ldots, p_{k-2}^w \vdash \varphi$ итд., до $\vdash \varphi$. □

▼ Задаци и додаци

1. Доказати:
(а) $\vdash_Ł (\alpha \Rightarrow \beta) \Rightarrow ((\alpha \Rightarrow \neg\beta) \Rightarrow \neg\alpha)$
(б) $\vdash_Ł (\alpha \Rightarrow (\beta \Rightarrow \alpha)) \Rightarrow (\beta \Rightarrow (\alpha \Rightarrow \beta))$

2. Кажемо да су скупови формула Γ_1 и Γ_2 Ł-еквивалентни, ако за сваку формулу α важи:

$$\Gamma_1 \vdash_Ł \alpha \text{ акко } \Gamma_2 \vdash_Ł \alpha.$$

Доказати да су $\{p_1, p_2, p_3\}$ и $\{p_1, p_1 \Rightarrow p_2, p_1 \Rightarrow (p_2 \Rightarrow p_3)\}$ Ł-еквивалентни скупови формула.

Додатак

Поред Лукасиевичевог рачуна Ł постоје и многе друге формалне теорије који описују таутологије исказне логике. Издвајамо формални систем који се назива *Хилбертов исказни рачун*.

Давид Хилберт (1862–1943) је био немачки матемартичар, један од најутицајнијих математичара своје епохе, који је дао велики допринос многим гранама математике.

- алфабет чине логички везници $\wedge$, $\vee$, $\Rightarrow$, $\neg$, логичка константа $\perp$, заграде (,) и исказна слова $p, q, r, \ldots, p_n, q_n, r_n, \ldots$;
- формуле су све исказне формуле изграђене на уобичајени начин (у којима се појављују само симболи уведеног алфабета);
- аксиоме су:

(H1)	$\varphi \Rightarrow (\psi \Rightarrow \varphi)$,	**(H2)**	$(\varphi \Rightarrow (\psi \Rightarrow \theta)) \Rightarrow ((\varphi \Rightarrow \psi) \Rightarrow (\varphi \Rightarrow \theta))$,
(H3)	$\varphi \wedge \psi \Rightarrow \varphi$,	**(H4)**	$\varphi \wedge \psi \Rightarrow \psi$,
(H5)	$\varphi \Rightarrow (\psi \Rightarrow \varphi \wedge \psi)$,	**(H6)**	$\varphi \Rightarrow \varphi \vee \psi$,
(H7)	$\psi \Rightarrow \varphi \vee \psi$,	**(H8)**	$(\varphi \Rightarrow \theta) \Rightarrow ((\psi \Rightarrow \theta) \Rightarrow (\varphi \vee \psi \Rightarrow \theta))$,
(H9)	$\neg\varphi \Rightarrow (\varphi \Rightarrow \bot)$,	**(H10)**	$(\varphi \Rightarrow \bot) \Rightarrow \neg\varphi$,
(H11)	$\bot \Rightarrow \varphi$,	**(H12)**	$\varphi \vee \neg\varphi$,

где су φ, ψ, θ произвољне формуле;

- једино правило извођења је модус поненс:

$$\frac{\varphi \qquad \varphi \Rightarrow \psi}{\psi}\ (MP)$$

где су φ, ψ произвољне формуле.

Ако у Хилбертовом исказном рачуну постоји извођење формуле φ из хипотеза Γ, пишемо $\Gamma \vdash_{\mathrm{H}} \varphi$.

Теорема дедукције. $\Gamma, \alpha \vdash_{\mathrm{H}} \beta$ акко $\Gamma \vdash_{\mathrm{H}} \alpha \Rightarrow \beta$

---

3. Доказати:
(а) $\alpha \Rightarrow \beta, \beta \Rightarrow \gamma, \vdash_{\mathrm{H}} \alpha \Rightarrow \gamma$
(б) $\Gamma \vdash_{\mathrm{H}} \neg\varphi$ акко $\Gamma, \varphi \vdash_{\mathrm{H}} \bot$

4. Доказати да су следеће формуле теореме у Хилбертовом исказном рачуну:

(а) $\alpha \Rightarrow \beta, \alpha \Rightarrow \gamma \vdash \alpha \Rightarrow (\beta \wedge \gamma)$;	(б) $\alpha \Rightarrow \beta, \alpha \wedge \beta \Rightarrow \gamma \vdash \alpha \Rightarrow \gamma$;
(в) $\alpha \Rightarrow (\beta \Rightarrow \gamma) \vdash \alpha \wedge \beta \Rightarrow \gamma$;	(г) $\alpha \Rightarrow (\beta \wedge \gamma) \vdash (\alpha \Rightarrow \beta) \wedge (\alpha \Rightarrow \beta)$;
(д) $\alpha, \alpha \Leftrightarrow \beta \vdash \beta$;	(ђ) $\alpha \wedge \beta \vdash \neg(\alpha \Rightarrow \neg\beta)$;
(е) $\neg(\alpha \Rightarrow \beta) \vdash \neg\beta$;	(ж) $\alpha \Rightarrow \beta \vdash \neg\beta \Rightarrow \neg\alpha$;
(з) $\neg\beta \Rightarrow \neg\alpha \vdash \alpha \Rightarrow \beta$;	(и) $\alpha \Rightarrow \beta \vdash \neg(\alpha \wedge \neg\beta)$;
(ј) $\alpha \Rightarrow \beta \vdash \neg\alpha \vee \beta$;	(к) $\alpha \vee \beta, \neg\alpha \vdash \beta$.

5. Сваку исказну формулу φ можемо трансформисати у еквивалентну формулу φ^* у којој се појављују само везници $\neg$ и $\Rightarrow$. Наравно, ако φ садржи само везнике $\neg$ и $\Rightarrow$, онда су φ и φ^* истоветне формуле. Доказати: $\vdash_{\mathrm{H}} \varphi$ акко $\vdash_{\text{Ł}} \varphi^*$.

$\{\neg, \Rightarrow\}$ је потпун систем исказних везника.

Додатак

Применом тврђења из претходног задатка и теореме потпуности за рачун Ł (страна 55), следи потпуност рачуна H: за сваку исказну формулу φ: $\vdash_{\mathrm{H}} \varphi$ акко $\models \varphi$. У наредним задацима, писаћемо само $\vdash$, при чему се подразумева индекс H. Очигледна последица теореме потпуности јесте: формула φ није доказива акко φ није таутологија. Штавише, применом теореме дедукције једноставно изводимо потребан и довољан услов да се нека формула не може извести из неког коначног скупа претпоставки. Прецизније из,

$p \Rightarrow (q \Rightarrow r) \equiv p \wedge q \Rightarrow r$

$$\begin{aligned} \alpha_1, \ldots, \alpha_n \vdash \varphi \quad &\text{акко} \quad \vdash \alpha_1 \Rightarrow (\alpha_2 \Rightarrow (\cdots(\alpha_n \Rightarrow \varphi)\cdots)) \\ &\text{акко} \quad \vdash \alpha_1 \wedge \cdots \wedge \alpha_n \Rightarrow \varphi \\ &\text{акко} \quad \models \alpha_1 \wedge \cdots \wedge \alpha_n \Rightarrow \varphi \end{aligned}$$

закључујемо

$$\begin{aligned}\alpha_1, \ldots, \alpha_n \not\vdash \varphi \quad & \text{акко} \quad \not\models \alpha_1 \wedge \cdots \wedge \alpha_n \Rightarrow \varphi \\ & \text{акко} \quad \text{постоји валуација таква да су} \\ & \qquad\quad \text{формуле } \alpha_1, \ldots, \alpha_n \text{ тачне,} \\ & \qquad\quad \text{а формула } \varphi \text{ нетачна.}\end{aligned}$$

---

6. Уписати знак $\times$ у квадратић испред формуле која се може извести из скупа $\{p \Rightarrow \neg q, r \Rightarrow q, p\}$:
$\square\ \neg(p \Rightarrow q)$ $\square\ q \Rightarrow \neg p$ $\square\ \neg p$

7. Уписати знак $\times$ у квадратић испред формуле која се се не може извести из скупа $\{p \Rightarrow q, \neg r \Rightarrow \neg q, p\}$:
$\square\ r \Rightarrow q$ $\square\ \neg q \Rightarrow \neg p$ $\square\ \neg r$

8. Скуп формула Γ је *независтан* ако за сваку формулу $\gamma \in \Gamma$ важи $\Gamma \setminus \{\gamma\} \not\vdash \gamma$.

Испитати који су од следећих скупова (p, q, r су исказна слова) независни:

- $\{p \Rightarrow q, q \Rightarrow r, r \Rightarrow p\}$;
- $\{p \Rightarrow q, q \Rightarrow r, p \Rightarrow r\}$;
- $\{p \vee q, p \Rightarrow r, q \Rightarrow r, \neg p \Rightarrow q \vee r\}$
- $\{p, q, p \Rightarrow r, r \Rightarrow q\}$.

2. Природна дедукција

Желео сам да конструишем формализам који ће бити близак, што је могуће више, стварном закључивању. Тако је настао рачун природне дедукције.

Герхард Генцен, цитат из његове докторске дисертације *Истраживања логичке дедукције* (Untersuchungen über das logische Schließen), одбрањене 1934. године

Готлоб Фреге (1848–1925) био је немачки математичар и филозоф. Сматра се једним од оснивача модерне математичке логике и аналитичке филозофије. Једно од најзначајнијих дела математичке логике је Фрегеова књига Begriffsschrift (*Појмовно писмо*), објављена 1879. године. Поднаслов овог дела је: *формални језик за чисто мишљење, по узору на језик аритметике.*

2.1 Исказна природна дедукција

Увод. У исказном рачуну Ł, доминантну улогу има импликација. Значај импликације још више долази до изражаја ако се примети да је $\{\Rightarrow, \perp\}$ потпун систем везника: $\neg\alpha \equiv \alpha \Rightarrow \perp$.

Главну улогу у извођењима у рачуну Ł имају:

- правило *модус поненс* $\dfrac{\alpha \quad \alpha \Rightarrow \beta}{\beta}$, које одређује како да користимо *импликације*, тј. формуле чији је главни знак $\Rightarrow$ и
- теорема дедукције – $\Gamma, \alpha \vdash \beta$ акко $\Gamma \vdash \alpha \Rightarrow \beta$; теорема дедукције омогућава да природно доказујемо *импликације*: да бисмо доказали $\Gamma \vdash \alpha \Rightarrow \beta$, довољно је доказати $\Gamma, \alpha \vdash \beta$.

Примену теореме дедукције можемо сажето приказати као правило следећег облика:

	Када желимо да докажемо $\alpha \Rightarrow \beta$:
α	уводимо додатну претпоставку α
$\vdots$	и настојимо да докажемо β.
β	Када успемо,
$\alpha \Rightarrow \beta$	изводимо закључак $\alpha \Rightarrow \beta$.

Примену овог правила илуструјемо извођењем следеће Ł-теореме $p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$.

		Да бисмо доказали $p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$ уводимо
1.	p	додатну претпоставку p.
		Настојимо да докажемо $(p \Rightarrow q) \Rightarrow q$, и зато уводимо и
2.	$p \Rightarrow q$	додатну претпоставку $p \Rightarrow q$.
3.	q	Применом (MP) на 1. и 2. добијамо q.
4.	$(p \Rightarrow q) \Rightarrow q$	Додавањем претпоставке $p \Rightarrow q$ доказано је q.
5.	$p \Rightarrow ((p \Rightarrow q) \Rightarrow q)$	Додавањем претпоставке p доказано је $(p \Rightarrow q) \Rightarrow q$.

Ова запажања веома су блиска идејама на којима је заснован једна од најпознатијих формалних теорија које карактеришу исказну логику – природна дедукција.

План

- основна правила природне дедукције: увођење и елиминација логичких везника, правило класичне непротивречности
- изведена правила: modus tolens, закони двојне негације, дисјунктивни силогизми, транзитивност импликације, закон контрапозиције, закон искључења трећег, ДеМорганови закони

Рачун природне дедукције увео је, 1935. године, Герхард Генцен са намером да природније опише уобичајено закључивање математичара. Скуп аксиома овог формалног система је празан док су правила извођења дата следећим схемама (у смислу да α, β и γ могу бити произвољне формуле):

$$\frac{\alpha \quad \beta}{\alpha \wedge \beta}\ (\wedge_{\mathrm{U}})$$

Увођење конјункције ($\wedge_{\mathrm{U}}$): из претпоставки α, β (директно) закључујемо $\alpha \wedge \beta$. Можемо размишљати и овако: да бисмо доказали $\alpha \wedge \beta$ потребно је да докажемо сваки конјункт појединачно, и α и β. Другим речима доказ за $\alpha \wedge \beta$ добијамо спајањем доказа за α и доказа за β.

$$\frac{\alpha \wedge \beta}{\alpha}\ (\wedge^{\mathrm{L}}_{\mathrm{E}}) \qquad \frac{\alpha \wedge \beta}{\beta}\ (\wedge^{\mathrm{D}}_{\mathrm{E}})$$

Елиминација конјункције: из претпоставке $\alpha \wedge \beta$ закључујемо α (одн. β) применом правила ($\wedge^{\mathrm{L}}_{\mathrm{E}}$) (одн. ($\wedge^{\mathrm{D}}_{\mathrm{E}}$)).

Пример 23. Докажимо секвент $(p \wedge q) \wedge s, r \wedge t \vdash t \wedge q$.

1.	$(p \wedge q) \wedge s$	претпоставка
2.	$r \wedge t$	претпоставка
3.	$p \wedge q$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 1
		[$p \wedge q$ је добијено применом правила $\wedge^{\mathrm{L}}_{\mathrm{E}}$ на 1.]
4.	q	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 3
5.	t	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 2
6.	$t \wedge q$	$\wedge_{\mathrm{U}}$, 5, 4

Наведени доказ можемо приказати и на следећи начин.

$$\dfrac{\dfrac{r \wedge t}{t}\,\wedge^{\mathrm{D}}_{\mathrm{E}} \qquad \dfrac{\dfrac{(p \wedge q) \wedge s}{p \wedge q}\,\wedge^{\mathrm{L}}_{\mathrm{E}}}{q}\,\wedge^{\mathrm{D}}_{\mathrm{E}}}{t \wedge q}\,\wedge_{\mathrm{U}}$$

За сваки исказни везник користимо две врсте правила. Правила увођења везника користимо да бисмо доказали сложене формуле са тим главним везником. Правила елиминације везника омогућавају да током извођења користимо сложене формуле са тим главним везником. У складу са тим, уводна разматрања најављују правила увођења и елиминације импликације.

$$\frac{\alpha \Rightarrow \beta \quad \alpha}{\beta}\ (\Rightarrow_{\mathrm{E}})$$

Елиминација импликације (одн. модус поненс) ($\Rightarrow_{\mathrm{E}}$) описује како се користе тврдње формулисане у облику имликације.

$$\frac{\left|\begin{array}{l}\alpha\\ \vdots\\ \beta\end{array}\right.}{\alpha \Rightarrow \beta}\ (\Rightarrow_{\mathrm{U}})$$

Увођење импликације ($\Rightarrow_{\mathrm{U}}$): да бисмо доказали импликацију $\alpha \Rightarrow \beta$ треба увести *додатну (привремену) претпоставку* α и доказати β, при чему је у том доказу дозвољено користити α, све остале претпоставке и међузакључке које смо већ извели. Доказ формуле β након увођења додатне претпоставке α истичемо вертикалном цртом и називамо *поддоказом*. Непосредно испод завршетка вертикалне линије наводимо закључак $\alpha \Rightarrow \beta$, ознаку правила ($\Rightarrow_{\mathrm{U}}$) и бројеве којима су нумерисани кораци поддоказа.

Пример 24. Докажимо $p \Rightarrow q, p \Rightarrow r \vdash p \Rightarrow q \wedge r$

1.	$p \Rightarrow q$	претпоставка
2.	$p \Rightarrow r$	претпоставка
3.	$\mid\ p$	додатна претпоставка
4.	$\mid\ q$	$\Rightarrow_E$, 1, 3
5.	$\mid\ r$	$\Rightarrow_E$, 2, 3
6.	$\mid\ q \wedge r$	$\wedge_U$, 4, 5
7.	$p \Rightarrow q \wedge r$	$\Rightarrow_U$, 3-6

$\vdots$			Када треба доказати $\alpha \Rightarrow \beta$:
$j.$	$\mid\ \alpha$		уводимо додатну претпоставку α
$\vdots$	$\mid\ \vdots$		и настојимо да докажемо β.
$k.$	$\mid\ \beta$		Када успемо,
$k+1.$	$\alpha \Rightarrow \beta$	$\Rightarrow_U$, j-k	изводимо жељени закључак.

Еквиваленција два исказа $\alpha \Leftrightarrow \beta$ јесте заправо конјункција две обратне импликације $(\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \alpha)$, па се правила **увођења** и **елиминације еквиваленције** сама намећу.

$$\frac{\alpha \Rightarrow \beta \quad \beta \Rightarrow \alpha}{\alpha \Leftrightarrow \beta}(\Leftrightarrow_U) \qquad \frac{\alpha \Leftrightarrow \beta}{\alpha \Rightarrow \beta}(\Leftrightarrow_E^{LD}) \qquad \frac{\alpha \Leftrightarrow \beta}{\beta \Rightarrow \alpha}(\Leftrightarrow_E^{DL})$$

Уз правила увођења и елиминације негације наводимо и тзв. *правило класичне непротивречности*. То правило, које означавамо $\bot_c$, одговара уобичајеном начину доказивања у математици који започињемо речима *претпоставимо супротно...*

$$\frac{\alpha \quad \neg\alpha}{\bot}(\neg_E)$$

Елиминација негације $(\neg_E)$: из претпоставки α, $\neg\alpha$ изводимо контрадикцију.

$$\frac{\begin{array}{|l} \alpha \\ \vdots \\ \bot \end{array}}{\neg\alpha}(\neg_U)$$

Увођење негације $(\neg_U)$: ако из α докажемо контрадикцију, онда закључујемо $\neg\alpha$.

$$\frac{\begin{array}{|l} \neg\alpha \\ \vdots \\ \bot \end{array}}{\alpha}(\bot_c)$$

Правило класичне непротивречности $(\bot_c)$: да бисмо доказали α, у класичној логици, довољно је извести контрадикцију из $\neg\alpha$.

Пример 25. Докажимо $\vdash (p \Rightarrow \bot) \Rightarrow \neg p$.

1.	$\mid\ p \Rightarrow \bot$	додатна претпоставка
2.	$\mid\mid\ p$	додатна претпоставка
3.	$\mid\mid\ \bot$	$\Rightarrow_E$, 1, 2
4.	$\mid\ \neg p$	$\neg_U$, 2-3
5.	$(p \Rightarrow \bot) \Rightarrow \neg p$	$\Rightarrow_U$, 1-4

Остављамо за вежбу доказ $\vdash (\neg p \Rightarrow \bot) \Rightarrow p$.

$$\frac{\alpha}{\alpha \vee \beta}(\vee_U^L) \qquad \frac{\beta}{\alpha \vee \beta}(\vee_U^D)$$

Увођење дисјункције: из α (тј. ако смо доказали α) изводимо закључак $\alpha \vee \beta$, за било коју формулу β, применом правила $(\vee_U^L)$; на исти начин, из β изводимо закључак $\alpha \vee \beta$, за било коју формулу α, применом правила $(\vee_U^D)$.

Елиминација дисјункције ($\vee_{\mathrm{E}}$) описује на који начин у доказима користимо формуле облика $\alpha \vee \beta$. Замислимо да желимо да докажемо γ претпостављајући $\alpha \vee \beta$. Будући да не знамо која је од формула α, β тачна (а једна мора бити), морамо спровести два одвојена доказа:

$$\frac{\alpha \vee \beta \quad \begin{array}{|c}\alpha\\ \vdots\\ \gamma\end{array} \quad \begin{array}{|c}\beta\\ \vdots\\ \gamma\end{array}}{\gamma}\,(\vee_{\mathrm{E}})$$

- Најпре, претпостављамо да је α тачно и доказујемо γ.
- Затим, претпостављамо да је β тачно и доказујемо γ.

На основу ова два доказа и претпоставке $\alpha \vee \beta$ закључујемо γ, јер два поддоказа покривају обе могућности.

Сва наведена правила карактеришу доказивост **секвената**

$$\varphi_1, \ldots, \varphi_k \vdash \psi$$

(тј. доказивост да из претпоставки $\varphi_1, \ldots, \varphi_k$ следи ψ). Секвенте доказујемо тако што формирамо низ који чине претпоставке $\varphi_1, \ldots, \varphi_k$ и (међу)закључци добијени применом правила дедукције на већ наведене формуле. Поступак завршавамо када добијемо жељени закључак ψ, а формирани низ називамо доказом формуле ψ из $\varphi_1, \ldots, \varphi_k$, одн. *доказом* одговарајућег секвента.

ПРИМЕР 26. Докажимо $\vdash (p \Rightarrow q) \vee (p \Rightarrow r) \Rightarrow (p \Rightarrow q \vee r)$.

1.	$(p \Rightarrow q) \vee (p \Rightarrow r)$	додатна претпоставка
2.	$p \Rightarrow q$	додатна претпоставка
3.	p	додатна претпоставка
4.	q	$\Rightarrow_{\mathrm{E}}$, 2, 3
5.	$q \vee r$	$\vee_{\mathrm{U}}^{\mathrm{L}}$, 4
6.	$p \Rightarrow (q \vee r)$	$\Rightarrow_{\mathrm{U}}$, 3-5
7.	$p \Rightarrow r$	додатна претпоставка
8.	p	додатна претпоставка
9.	r	$\Rightarrow_{\mathrm{E}}$, 7, 8
10.	$q \vee r$	$\vee_{\mathrm{U}}^{\mathrm{D}}$, 9
11.	$p \Rightarrow (q \vee r)$	$\Rightarrow_{\mathrm{U}}$, 8-10
12.	$p \Rightarrow (q \vee r)$	$\vee_{\mathrm{E}}$, 1, 2-6, 7-11
13.	$(p \Rightarrow q) \vee (p \Rightarrow r) \Rightarrow (p \Rightarrow q \vee r)$	$\Rightarrow_{\mathrm{U}}$, 1-12

Да бисмо поједноставили доказивање секвената, списак правила проширујемо још неким **изведеним правилима**, чија се употреба, наравно, једноставно може елиминисати из сваког доказа.

$$\frac{\alpha \Rightarrow \beta \quad \neg\beta}{\neg\alpha}\ (\mathrm{MT})$$

Правило modus tolens (MT) може бити веома корисно при употреби тврдњи у облику импликације.

1.	$\alpha \Rightarrow \beta$	претпоставка
2.	$\neg\beta$	претпоставка
3.	$\mid\ \alpha$	додатна прет.
4.	$\mid\ \beta$	$\Rightarrow_{\mathrm{E}}$, 1, 3
5.	$\mid\ \bot$	$\neg_{\mathrm{E}}$, 4, 2
6.	$\neg\alpha$	$\neg_{\mathrm{U}}$, 3-5

$$\frac{\neg\neg\alpha}{\alpha}\ (\neg\neg_{\mathrm{E}}) \qquad \frac{\alpha}{\neg\neg\alpha}\ (\neg\neg_{\mathrm{U}})$$

Правило $(\neg\neg_{\mathrm{E}})$ нам дозвољава да обришемо два знака негације. Насупрот томе, правило $(\neg\neg_{\mathrm{U}})$ дозвољава да се испред сваке формуле допишу два знака негације. Оправдавамо само правило $\neg\neg_{\mathrm{U}}$.

1.	α	претпоставка
2.	$\mid\ \neg\alpha$	додатна прет.
3.	$\mid\ \bot$	$\neg_{\mathrm{E}}$, 1, 2
4.	$\neg\neg\alpha$	$\neg_{\mathrm{U}}$, 2-3

Пример 27. Примену изведених правила можемо елиминисати из сваког доказа. То ћемо илустровати извођењем секвента $p \Rightarrow \neg q, q \vdash \neg p$ на два начина. Прво наводимо извођење секвента користећи изведена правила $\neg\neg_{\mathrm{U}}$ и MT.

1.	$p \Rightarrow \neg q$	претпоставка
2.	q	претпоставка
3.	$\neg\neg q$	$\neg\neg_{\mathrm{U}}$, 2
4.	$\neg p$	MT, 1, 3

Дати секвент доказујемо и без правила $\neg\neg_{\mathrm{U}}$ и MT.[70]

1.	$p \Rightarrow \neg q$	претпоставка
2.	q	претпоставка
3.	$\mid\ \neg q$	додатна претпоставка
4.	$\mid\ \bot$	$\neg_{\mathrm{E}}$, 2, 3
5.	$\neg\neg q$	$\neg_{\mathrm{U}}$, 3-4
6.	$\mid\ p$	додатна претпоставка
7.	$\mid\ \neg q$	$\Rightarrow_{\mathrm{E}}$, 1, 6
8.	$\mid\ \bot$	$\neg_{\mathrm{E}}$, 2, 7
9.	$\neg p$	$\neg_{\mathrm{U}}$, 6-8

[70] Примену правила $\neg\neg_{\mathrm{U}}$ и MT елиминишемо навођењем извођења тих правила из основних правила.

Транзитивност импликације	Закони контрапозиције	
$\dfrac{\alpha \Rightarrow \beta \quad \beta \Rightarrow \gamma}{\alpha \Rightarrow \gamma}$ (T)	$\dfrac{\alpha \Rightarrow \beta}{\neg\beta \Rightarrow \neg\alpha}$ (K)	$\dfrac{\neg\alpha \Rightarrow \neg\beta}{\beta \Rightarrow \alpha}$ (K)

1.	$\alpha \Rightarrow \beta$	претпоставка
2.	$\beta \Rightarrow \gamma$	претпоставка
3.	$\mid\ \alpha$	додатна прет.
4.	$\mid\ \beta$	$\Rightarrow_{\mathrm{E}}$, 1, 3
5.	$\mid\ \gamma$	$\Rightarrow_{\mathrm{E}}$, 2, 4
6.	$\alpha \Rightarrow \gamma$	$\Rightarrow_{\mathrm{U}}$, 3-5

1.	$\alpha \Rightarrow \beta$	претпоставка
2.	$\mid\ \neg\beta$	додатна прет.
3.	$\mid\ \neg\alpha$	MT, 1, 2
4.	$\neg\beta \Rightarrow \neg\alpha$	$\Rightarrow_{\mathrm{U}}$, 2-3

Ex falso quodlibet
$\dfrac{\bot}{\varphi}(\bot_E)$

Правило $(\bot_E)$ се непосредно добија из $(\bot_c)$. Правило $(\bot_E)$ је познато и као *принцип дедуктивне експлозије* (из контрадикције следи све).

Дисјунктивни силогизми	
$\dfrac{\alpha \vee \beta \quad \neg\alpha}{\beta}$ (DS)	$\dfrac{\alpha \vee \beta \quad \neg\beta}{\alpha}$ (DS)

1.	$\alpha \vee \beta$	претпоставка
2.	$\neg\alpha$	претпоставка
3.	α	додатна претпоставка
4.	$\bot$	$\neg_E$, 3, 2
5.	β	$\bot_E$, 4
6.	β	додатна претпоставка
7.	β	$\vee_E$, 1, 3-5, 6

Закон искључења трећег
$\dfrac{}{\alpha \vee \neg\alpha}$ (TND)

Према закону искључења трећег, у доказима можемо користити као претпоставку $\alpha \vee \neg\alpha$, за било коју формулу α.

1.	$\neg(\alpha \vee \neg\alpha)$	додатна претпоставка
2.	α	додатна претпоставка
3.	$\alpha \vee \neg\alpha$	$\vee_U^L$, 2
4.	$\bot$	$\neg_E$, 1, 3
5.	$\neg\alpha$	$\neg_U$, 2-4
6.	$\alpha \vee \neg\alpha$	$\vee_U^D$, 5
7.	$\bot$	$\neg_E$, 1, 6
8.	$\alpha \vee \neg\alpha$	$\bot_c$, 1-7

Де Моргановини закони			
$\dfrac{\neg\alpha \vee \neg\beta}{\neg(\alpha \wedge \beta)}$ (DM)	$\dfrac{\neg\alpha \wedge \neg\beta}{\neg(\alpha \vee \beta)}$ (DM)	$\dfrac{\neg(\alpha \vee \beta)}{\neg\alpha \wedge \neg\beta}$ (DM)	$\dfrac{\neg(\alpha \wedge \beta)}{\neg\alpha \vee \neg\beta}$ (DM)

Свако од ова четири правила назваћемо Де Моргановим законом, јер приликом примене неће бити забуне.

1.	$\neg\alpha \vee \neg\beta$	претпоставка	1.	$\neg\alpha \wedge \neg\beta$	претпоставка
2.	$\alpha \wedge \beta$	додатна прет.	2.	$\neg\alpha$	$\wedge_E^L$, 1
3.	α	$\wedge_E^L$, 2	3.	$\neg\beta$	$\wedge_E^D$, 1
4.	$\neg\neg\alpha$	$\neg\neg_U$,	4.	$\alpha \vee \beta$	додатна прет.
5.	$\neg\beta$	DS, 1, 4	5.	β	DS, 4, 2
6.	β	$\wedge_E^D$, 2	6.	$\bot$	$\neg_E$, 5, 3
7.	$\bot$	$\neg_E$, 6, 5	7.	$\neg(\alpha \vee \beta)$	$\neg_U$, 2-6
8.	$\neg(\alpha \wedge \beta)$	$\neg_U$, 2-7			

1.	$\neg(\alpha\vee\beta)$	претпоставка
2.	α	додатна прет.
3.	$\alpha\vee\beta$	$\vee^{\mathrm{L}}_{\mathrm{U}}$, 2
4.	$\bot$	$\neg_{\mathrm{E}}$, 3, 1
5.	$\neg\alpha$	$\neg_{\mathrm{U}}$, 2-4
6.	β	додатна прет.
7.	$\alpha\vee\beta$	$\vee^{\mathrm{D}}_{\mathrm{U}}$, 6
8.	$\bot$	$\neg_{\mathrm{E}}$, 7, 1
9.	$\neg\beta$	$\neg_{\mathrm{U}}$, 6-8
10.	$\neg\alpha\wedge\neg\beta$	$\wedge_{\mathrm{U}}$, 5, 9

1.	$\neg(\alpha\wedge\beta)$	претпоставка
2.	$\alpha\vee\neg\alpha$	TND
3.	α	додатна прет.
4.	β	додатна прет.
5.	$\alpha\wedge\beta$	$\wedge_{\mathrm{U}}$, 3, 4
6.	$\bot$	$\neg_{\mathrm{E}}$, 5, 1
7.	$\neg\beta$	$\neg_{\mathrm{U}}$, 4-6
8.	$\neg\alpha\vee\neg\beta$	$\vee^{\mathrm{D}}_{\mathrm{U}}$, 7
9.	$\neg\alpha$	додатна прет.
10.	$\neg\alpha\vee\neg\beta$	$\vee^{\mathrm{L}}_{\mathrm{U}}$, 9
11.	$\neg\alpha\vee\neg\beta$	$\vee_{\mathrm{E}}$, 2, 3-8, 9-10

Систем природне дедукције је такође потпун. Овај доказ изостављамо, јер је заснован на сличним идејама као доказ теорема потпуности и сагласности за исказни рачун Ł.

Теорема 10. *Секвент* $\vdash\varphi$ *је доказив применом правила природне дедукције акко је* φ *таутологија.*

▼ Задаци и додаци

Основна правила исказне природне дедукције

$$\frac{\alpha\wedge\beta}{\alpha}\,(\wedge^{\mathrm{L}}_{\mathrm{E}})\qquad \frac{\alpha\wedge\beta}{\beta}\,(\wedge^{\mathrm{D}}_{\mathrm{E}})\qquad \frac{\alpha\quad\beta}{\alpha\wedge\beta}\,(\wedge_{\mathrm{U}})$$

$$\frac{\alpha\Rightarrow\beta\quad\alpha}{\beta}\,(\Rightarrow_{\mathrm{E}})\qquad \frac{\begin{array}{|l}\alpha\\ \vdots\\ \beta\end{array}}{\alpha\Rightarrow\beta}\,(\Rightarrow_{\mathrm{U}})\qquad \frac{\alpha\Rightarrow\beta\quad\beta\Rightarrow\alpha}{\alpha\Leftrightarrow\beta}\,(\Leftrightarrow_{\mathrm{U}})\qquad \frac{\alpha\Leftrightarrow\beta}{\alpha\Rightarrow\beta}\,(\Leftrightarrow^{\mathrm{LD}}_{\mathrm{E}})\qquad \frac{\alpha\Leftrightarrow\beta}{\beta\Rightarrow\alpha}\,(\Leftrightarrow^{\mathrm{DL}}_{\mathrm{E}})$$

$$\frac{\alpha\quad\neg\alpha}{\bot}\,(\neg_{\mathrm{E}})\qquad \frac{\begin{array}{|l}\alpha\\ \vdots\\ \bot\end{array}}{\neg\alpha}\,(\neg_{\mathrm{U}})\qquad \frac{\begin{array}{|l}\neg\alpha\\ \vdots\\ \bot\end{array}}{\alpha}\,(\bot_{\mathrm{c}})$$

$$\frac{\alpha}{\alpha\vee\beta}\,(\vee^{\mathrm{L}}_{\mathrm{U}})\qquad \frac{\beta}{\alpha\vee\beta}\,(\vee^{\mathrm{D}}_{\mathrm{U}})\qquad \frac{\alpha\vee\beta\quad \begin{array}{|l}\alpha\\ \vdots\\ \gamma\end{array}\quad \begin{array}{|l}\beta\\ \vdots\\ \gamma\end{array}}{\gamma}\,(\vee_{\mathrm{E}})$$

1. Користећи само основна правила природне дедукције, доказати:

(а) $p\wedge q\Rightarrow r, r\Rightarrow s, q\wedge\neg s\vdash\neg p$
(б) $p, p\vee q\Rightarrow\neg s, r\Rightarrow s\vdash\neg r$
(в) $p\vee q, p\vee r, \neg q\vee\neg r\vdash p$
(г) $\neg p\vee r, \neg q\vee r, p\vee q\vdash r$
(д) $\vdash p\Rightarrow(q\Rightarrow p)$
(ђ) $\vdash(p\Rightarrow q)\wedge(p\Rightarrow r)\Rightarrow(p\Rightarrow q\wedge r)$
(е) $\vdash(p\Rightarrow q)\wedge(r\Rightarrow q)\Rightarrow(p\vee r\Rightarrow q)$
(ж) $p\Rightarrow q, p\wedge q\Rightarrow r\vdash p\Rightarrow r$
(з) $p\Rightarrow(q\Rightarrow r)\vdash p\wedge q\Rightarrow r$
(и) $p\Rightarrow q\vdash\neg(p\wedge\neg q)$

2. Доказати следеће секвенте:

(а) $\neg p\Rightarrow q, \neg p\vee(\neg q\Rightarrow r), \neg q\vdash r$
(б) $\neg p\vee q\Rightarrow r, s\vee\neg q, \neg t, p\Rightarrow t, \neg p\wedge r\Rightarrow\neg s\vdash\neg q$
(в) $p\wedge q\Rightarrow r, r\Rightarrow s, q\wedge\neg s\vdash\neg p$

$p \Rightarrow q, r \vee s, \neg s \Rightarrow \neg t, \neg q \vee s, \neg s, \neg p \wedge r \Rightarrow u, w \vee t \vdash u \wedge w$

$c \vee e \Rightarrow \neg m, r \Rightarrow m, c \vdash \neg r$

$\neg a \Rightarrow (b \Rightarrow \neg c), c \Rightarrow \neg a, \neg d \vee a \Rightarrow c, \neg d \vdash \neg b$

$e \Rightarrow f, \neg g \Rightarrow \neg f, h \Rightarrow i, e \vee h \vdash g \vee i$

3. Доказати:

$(\mathbf{A}^{\vee}) \vdash \alpha \vee (\beta \vee \gamma) \Leftrightarrow (\alpha \vee \beta) \vee \gamma$	$(\mathbf{A}^{\wedge}) \vdash \alpha \wedge (\beta \wedge \gamma) \Leftrightarrow (\alpha \wedge \beta) \wedge \gamma$
$(\mathbf{K}^{\vee}) \vdash \alpha \vee \beta \Leftrightarrow \beta \vee \alpha$	$(\mathbf{K}^{\wedge}) \vdash \alpha \wedge \beta \Leftrightarrow \beta \wedge \alpha$
$(\mathbf{D}^{\vee}_{\wedge}) \vdash \alpha \vee (\beta \wedge \gamma) \Leftrightarrow (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$	$(\mathbf{D}^{\wedge}_{\vee}) \vdash \alpha \wedge (\beta \vee \gamma) \Leftrightarrow (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$
$(\mathbf{C}^{\vee}) \vdash \alpha \vee \neg\alpha \Leftrightarrow \top$	$(\mathbf{C}^{\wedge}) \vdash \alpha \wedge \neg\alpha \Leftrightarrow \bot$
$(\mathbf{N}^{\vee}) \vdash \alpha \vee \bot \Leftrightarrow \alpha$	$(\mathbf{N}^{\wedge}) \vdash \alpha \wedge \top \Leftrightarrow \alpha$

4. (а) Доказати природном дедукцијом:

$$a, b \Rightarrow \neg a \wedge c, \neg b \wedge c \Rightarrow \neg a \vdash \neg b \wedge \neg c$$

(б) На суђењу особама A, B, C, D и E, осумњиченим за исти злочин, утврђене су следеће чињенице:

(1) Ако није крив D и јесте крив A, онда је крив и C.
(2) Ако је крив B, онда није крив A и јесте крив C.
(3) Ако није крив E и јесте крив A, онда није крив D.
(4) Ако није крив B и јесте крив C, онда није крив A.
(5) Осумњичени A јесте крив.

Да ли је још неко крив осим особе A?

5. (а) Доказати секвент: $a \vee b \Leftrightarrow \neg a \vdash \neg a \wedge b$.

(б) Аладин се налази испред две пећине A и B. На улазу у пећину A пише 'у једној од нас крије се благо', а на улазу у B 'у A нема блага'. Аладин зна да су обе изјаве тачне или су обе лажне. У којој пећини се налази благо?

6. Правила извођења *интуиционистичке* логике су сва правила класичне логике, **осим** правила $(\bot_{\mathrm{c}})$, које је замењено правилом $(\bot_{\mathrm{E}})$,

$$\frac{\bot}{\alpha} \quad (\bot_{\mathrm{E}}).$$

Са $\Gamma \vdash_{\mathrm{i}} \varphi$ означавамо чињеницу да се секвент $\Gamma \vdash \varphi$ може доказати применом само правила интуиционистичке логике.

Доказати:

(а) $\vdash_{\mathrm{i}} (\neg\neg\alpha \Rightarrow \neg\neg\beta) \Rightarrow \neg\neg(\alpha \Rightarrow \beta)$;
(б) $\vdash_{\mathrm{i}} \neg\neg((\neg\beta \Rightarrow \neg\alpha) \Rightarrow (\alpha \Rightarrow \beta))$;
(в) $\vdash_{\mathrm{i}} \neg\neg(((\alpha \Rightarrow \beta) \Rightarrow \alpha) \Rightarrow \alpha)$;
(г) $\vdash_{\mathrm{i}} \neg\neg((\alpha \wedge \beta \Rightarrow \gamma) \Rightarrow (\alpha \Rightarrow \gamma) \vee (\beta \Rightarrow \gamma))$;
(д) $\vdash_{\mathrm{i}} \neg\neg((\alpha \Rightarrow \beta \vee \gamma) \Rightarrow (\alpha \Rightarrow \beta) \vee (\alpha \Rightarrow \gamma))$;
(ђ) $\vdash_{\mathrm{i}} \neg\neg((\alpha \Rightarrow \beta) \vee (\beta \Rightarrow \alpha))$.

2.2 Чист предикатски језик

Увод. Неформално говорећи, исказне формуле описују структуру реченица узимајући у обзир само начин на који су неки једноставни искази повезани логичким везницима, док је значење тих полазних исказа потпуно неважно. Тако, исказне формуле нису довољно изражајне да би се помоћу њих анализирало и разматрало следеће чувено закључивање:

> Сваки човек је смртан.
> Сократ је човек.
> **Дакле**, Сократ је смртан.

Предикатска језик омогућава да разматрамо и смисао исказа. Пре него што детаљно опишемо овај језик, неке полазне идеје илустроваћемо примерима блиским говорном језику, али у контексту који је донекле ведрији од оног на који се односи претходно закључивање.

Природни језици нису погодни за прецизно изражавање смисла исказа. Да ли реченица *Сваки момак воли једну девојку* значи: (1) *Постоји једна девојка коју воли сваки момак* или (2) *За сваког момка се може пронаћи једна девојка коју он воли*?

Потреба да се елиминишу двосмислености природног језика довела је, између осталог, до увођења тзв. *формалних језика* чије се реченице формирају према унапред утврђеним правилима. Реченице (1) и (2) формално ћемо изразити користећи:

- логичке везнике ($\vee$, $\wedge$, $\neg$, $\Rightarrow$, $\Leftrightarrow$),
- квантификаторе $\forall$ – *сваки* и $\exists$ – *неки*,
- променљиве $x, y, z, x_1, y_1, z_1, x_2, \ldots$ (којима ћемо означавати 'произвољно', 'неодређено' људско биће) и
- помоћне знаке: зарез и заграде.

Поред тога, потребно је да неким симболима означимо и особине *бити момак* и *бити девојка*, као и однос *волети*. Изјаву '*x је момак*' означавамо $M(x)$, '*x је девојка*' означавамо $D(x)$, док $V(x,y)$ значи '*x воли y*'.

Реченицама (1) и (2) редом одговарају следеће формуле:

$$\exists x(D(x) \wedge \forall y(M(y) \Rightarrow V(y,x))) \quad \text{и} \quad \forall x(M(x) \Rightarrow \exists y(D(y) \wedge V(x,y))),$$

Још неколико реченица природног језика преводимо у формуле:

- Свако воли некога – $\forall x \exists y V(x,y)$
- Неко воли свакога – $\exists x \forall y V(x,y)$
- Неко не воли никога – $\exists x \forall y \neg V(x,y)$

План
- чист предикатски језик; предикатски симболи и симболи константи
- атомске формуле; предикатске формуле

Предикатски језик развијен је у једном од најважнијих дела савремене логике – у књижици Begriffsschrift (Појмовно писмо) од осамдесетак страница које је написао Готлоб Фреге и објавио 1879. године[71]. Поднаслов овог дела је: *формални језик за чисто мишљење, по узору на језик аритметике*.

Уопштено говорећи, чист предикатски језик описује извесне објекте помоћу унапред изабраних *предиката*. Сваки изабрани предикат представља једно својство низова објеката одређене дужине. Избором константи одређујемо универзум о коме говоримо, а избором предиката бирамо основне (атомске) исказе које користимо приликом описивања тог универзума.

[71] Фрегеа је, по сопственом признању, водила Лајбницова (1646–1716) идеја о универзалном језику, lingua charactera, чији је успех лежао у добром избору симбола. Фрегеов језик је вештачки језик одређен прецизним граматичким правилима, односно синтаксом. Слободно се може сматрати да је Begriffsschrift претеча програмских језика.

Алфабет чисте предикатске логике чине:

- **нелогички симболи** које бирамо у складу са контекстом;
  – *симболи константи*, тј. ознаке/имена објеката универзума који разматрамо;
  – *симболи предиката*, тј. ознака/имена за својства (осбине) низова објеката, при чему сваки предикат има своју дужину која представља број објеката на који се предикат односи.

ПРЕТХОДНИ ПРИМЕР:

Ако универзум чине сви људи, свака конкретна особа представља неку константу тог универзума: `Abelar`, `Eloiza` итд.
На пример, бирамо два унарна предиката M и D и један бинарни предикат V на универзуму људи, имајући на уму следећа значења:

$M(\cdot)$	бити момак
$D(\cdot)$	бити девојка
$V(\cdot,\cdot)$	волети

- **логички симболи**, које користимо у било ком контексту,
  – променљиве $x, y, z, x_1, y_1, z_1, \ldots$;
  – логички везници: $\wedge$, $\vee$, $\neg$, $\Rightarrow$ и $\Leftrightarrow$;
  – логичке константе: $\bot$, $\top$;
  – квантификатори: $\forall$ (универзални) и $\exists$ (егзистенцијални);
  – помоћни знаци, тј. уобичајени симболи за запету и заграде.

Предикатске формуле дефинишемо индуктивно полазећи од најједноставнијих тзв. атомских формула.

Атомску формулу одређују предикатски симбол и низ променљивих и/или константи одговарајуће дужине.

Атомске формуле у којима нема променљивих имају структуру најтипичнијих реченица говорног језика:

$M(\texttt{Abelar})$	Абелар је момак.
$D(\texttt{Eloiza})$	Елоиза је девојка.
$V(\texttt{Abelar},\texttt{Eloiza})$	Абелар воли Елоизу.
$V(\texttt{Eloiza},\texttt{Abelar})$	Елоиза воли Абелара.

Атомске формуле могу да садрже и променљиве: $M(x)$, $V(z,\texttt{Eloiza})$, $V(y,x)$ итд.

Предикатске формуле се граде применом следећих правила:

– логичке константе $\bot$ и $\top$, и све атомске формуле јесу формуле;

– ако је α формула, онда је и $\neg\alpha$ формула;

– ако су α и β формуле, онда су $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \Rightarrow \beta)$, $(\alpha \Leftrightarrow \beta)$ такође формуле;

– ако је α формула и x променљива, онда су $\forall x\alpha$ и $\exists x\alpha$ формуле.

$\neg D(\texttt{Abelar})$
$V(\texttt{Eloiza}, x) \Rightarrow \neg V(x, \texttt{Eloiza})$
$D(x) \wedge \neg D(y) \Rightarrow V(x, y) \vee V(y, x)$
$\forall x\, V(x, \texttt{Eloiza})$
$\exists z\, V(\texttt{Abelar}, z)$
$\forall x\, (V(x, \texttt{Ana}) \vee V(\texttt{Ana}, x))$
$\forall x\, V(x, \texttt{Ana}) \vee \forall x V(\texttt{Ana}, x)$
$\forall x \exists y\, V(x, y)$
$\exists y \forall x\, V(x, y)$
$\exists x(V(x, y) \Rightarrow M(x) \vee D(y)) \wedge \neg\forall y V(y, y)$

Када квантификатор са неком променљивом поставимо испред формуле, тада сва појављивања те променљиве у поменутој формули постају *везана* и кажемо да су под *дејством постављеног квантификатора*. Уколико неко појављивање променљиве у формули није под дејством ниједног квантификатора, кажемо да је *слободно*.

Променљива је **слободна** у некој формули ако има слободно појављивање у тој формули. Када желимо да истакнемо да су све слободне променљиве формуле α неке (не нужно све) од променљивих $x_1, \ldots, x_n$, онда пишемо $\alpha(x_1, \ldots, x_n)$.

Стрелице на слици показују на слободна појављивања променљивих.

$$\exists x(V(x, \overset{\downarrow}{y}) \Rightarrow M(x) \vee D(\overset{\downarrow}{y})) \wedge \neg\forall y V(y, y)$$

Појављивања осталих променљивих су везана.

Ако је α формула

$$\exists x(V(x, y) \Rightarrow M(x) \vee D(y)) \wedge \neg\forall y V(y, y)$$

онда бисмо је, ради истицања слободних променљивих, могли означити $\alpha(y)$, али и $\alpha(y, z)$, $\alpha(y, x_1, \ldots, x_n)$ и слично – важно је само да се променљива y појави на списку променљивих у загради.

Формула у којој променљиве немају слободна појављивања назива се **реченица**.

Истинитосне вредности формула су потпуно одређене када је позната:

- *валуацију атомских реченица*[72], тј. истинитосне вредности атомских реченица (атомске реченице можемо посматрати као исказна слова којима додељујемо истинитосне вредности 1 (тачно) или 0 (нетачно));
- *валуацију променљивих*, при чему вредност променљиве представља неки објекат универзума.

[72] Валуација атомских речени[...] се назива и *интерпретација* *не*[...] *гичких симбола*.

Истинитосну вредност било које формуле добијамо применом истинитосних таблица за логичке везнике и следећих правила за квантификаторе:

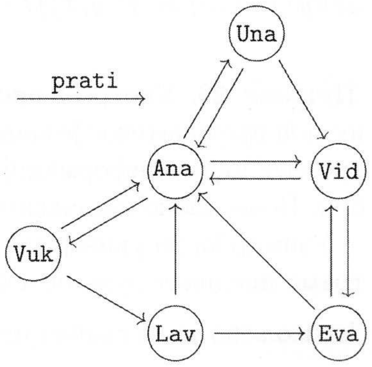
– формула $\forall x\alpha$ је тачна ако је за **сваки** (било који) објекат универзума додељен променљивој x формула α тачна;

$\forall x\alpha(x)$ је тачно, ако је $\alpha(c)$ [...]чно, за сваки објекат c универ[...]ма.

– формула $\exists x\alpha$ је тачна ако је за **неки** (бар један) објекат универзума додељен променљивој x формула α тачна.

$\exists x\alpha(x)$ је тачно, ако је $\alpha(c)$ тачно, за неки објекат c универзума.

Пример 28. На дијаграму десно приказано је шест особа и њихово међусобно праћење на некој друштвеној мрежи.



Универзум чине: Ana, Eva, Lav, Una, Vid, Vuk. Везе међу објектима универзума изражавамо бинарним предикатом $P(\cdot,\cdot)$ (коме одговара предикат говорног језика: '*прати*' или '*је пратилац*').

Дијаграм дефинише валуацију свих атомских формула. На пример, истинитосна вредност реченице $P(\texttt{Ana},\texttt{Eva})$ је 0, јер *Ана не прати Еву*; истинитосна вредност реченице $P(\texttt{Eva},\texttt{Ana})$ је 1, јер *Ева прати Ану*. Истинитост свих атомских реченица можемо приказати и табелом:

	Ana	Eva	Lav	Una	Vid	Vuk
Ana	0	0	0	1	1	1
Eva	1	0	0	0	1	0
Lav	1	1	0	0	0	0
Una	1	0	0	0	1	0
Vid	1	1	0	0	0	0
Vuk	1	0	1	0	0	0

Користећи истинитосне таблице исказних везника једноставно одређујемо истинитосну вредност нпр. реченице

$$P(\texttt{Eva},\texttt{Ana}) \land \neg P(\texttt{Ana},\texttt{Vid}) \Rightarrow \neg(P(\texttt{Vuk},\texttt{Vuk}) \lor P(\texttt{Una},\texttt{Lav}));$$

истинитосна вредност ове реченица је 1, тј. реченица је тачна:

$$1 \land \neg 1 \Rightarrow \neg(0 \lor 0) = 1.$$

Истинитосна вредност формуле са променљивама се може одредити само када је позната и валуација променљивих.

x	Ana	Eva	Lav	Una	Vid	Vuk
$P(\texttt{Ana}, x)$	0	0	0	1	1	1
$P(x,\texttt{Ana}) \lor P(x,\texttt{Una})$	1	1	1	1	1	1
$P(x,\texttt{Una}) \land P(\texttt{Lav}, x)$	1	0	0	0	0	0
$P(x,\texttt{Una}) \Rightarrow \neg P(\texttt{Lav}, x)$	0	1	1	1	1	1
$P(x,x)$	0	0	0	0	0	0

Из претходне табеле даље закључујемо да су тачне нпр. следеће реченице са квантификаторима:

$$\begin{array}{ll} \exists x\, P(\texttt{Ana}, x) & \neg\forall x\, P(\texttt{Ana}, x) \\ \exists x\,(P(x,\texttt{Ana}) \lor P(x,\texttt{Una})) & \forall x\,(P(x,\texttt{Ana}) \lor P(x,\texttt{Una})) \\ \neg\exists x\, P(x,x) & \neg\forall x\, P(x,x) \end{array}$$

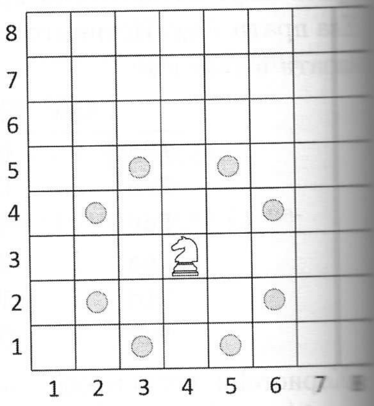
Било би веома заморно рачунати истинитосну вредност реченице

$$(*) \qquad \exists x \forall y\,(P(y,x) \Rightarrow P(x,y)),$$

разматрајући истиност формуле $P(y,x) \Rightarrow P(x,y)$ за све могуће вредности променљивих. Једноставније је реченицу $(*)$ превести

на говорни језик: *постоји особа која прати сваког свог пратиоца*, и пажљивом анализом дијаграма потражити загонетну особу. Није тешко уочити да Уна и Вук прате сваког свог пратиоца, одакле се закључује да је реченица $(*)$ тачна. Да ли је тачна реченица $\exists x \forall y\,(P(x,y) \Rightarrow P(y,x))$?

Пример 29. Употреба промењљивих значајно повећава изражајну моћ предикатског језика. Значај променљивих илуструјемо репрезентацијом информација о кретању скакача на шаховској табли. Поља табле означавамо паром бројева од 1 до 8.



Узимајући да универзум чине бројеви 1, 2, 3, 4, 5, 6, 7, 8; посматрамо предикат дужине 4 (тј. 4-арни предикат): $S(x_1, x_2, x_3, x_4)$

'дозвољено је да скакач пређе са поља (x_1, x_2) на поље (x_3, x_4).'

Један начин да наведемо све допустиве потезе јесте да их експлицитно набројимо:

$$(*) \quad S(1,1,2,3), S(1,1,3,2), \ldots$$

Листа је прилично дугачка и садржи 336 чињеница. Ситуацију можемо поправити, и листу знатно скратити ако опишемо неке опште чињенице о кретању скакача. На пример, следеће својство симетричности скраћује горњу листу на пола:

$$(\sigma_1)\ \forall x_1 \forall x_2 \forall x_3 \forall x_4 (S(x_1, x_2, x_3, x_4) \Rightarrow S(x_3, x_4, x_1, x_2)).$$

Уз додатне опште услове, може се изоставити још више појединачних чињеница листе $(*)$.

$$(\sigma_2)\ \forall x_1 \forall x_2 \forall x_3 \forall x_4 (S(x_1, x_2, x_3, x_4) \Rightarrow S(x_1, x_4, x_3, x_2))$$

$$(\sigma_3)\ \forall x_1 \forall x_2 \forall x_3 \forall x_4 (S(x_1, x_2, x_3, x_4) \Rightarrow S(x_2, x_1, x_4, x_3))$$

$$(\sigma_4)\ \forall x_1 \forall x_2 \forall x_3 \forall x_4 (S(x_1, x_2, x_3, x_4) \Rightarrow S(x_3, x_2, x_1, x_4))$$

Интуитивно је јасно да из $S(4,3,5,1)$,
- на основу (σ_1) закључујемо $S(4,1,5,3)$;
- на основу (σ_2) закључујемо $S(5,1,4,3)$;
- на основу (σ_3) закључујемо $S(3,4,1,5)$;
- на основу (σ_4) закључујемо $S(5,3,4,1)$.

Пример 30. Нека универзум чине бројеви: 0, 1, 2, 3, 4, 5, 6, 7. Бинарни предикат '... мањи од ...' означавамо $<$, и користимо тзв. *инфиксну* нотацију: пишемо $x < y$ уместо $<(x, y)$.

$<$	0	1	2	3	4	5	6	7
0	0	1	1	1	1	1	1	1
1	0	0	1	1	1	1	1	1
2	0	0	0	1	1	1	1	1
3	0	0	0	0	1	1	1	1
4	0	0	0	0	0	1	1	1
5	0	0	0	0	0	0	1	1
6	0	0	0	0	0	0	0	1
7	0	0	0	0	0	0	0	0

Уместо навођења истинитости сваког од 64 исказа, приказаних у табели десно, довољно је навести следећих девет конкретних веза

$$(*) \quad 0 < 1,\ 1 < 2,\ 2 < 3,\ 3 < 4,\ 4 < 5,\ 5 < 6,\ 6 < 7.$$

и неколико општих особина:

(O_1) $\forall x \neg x < x$

(O_2) $\forall x \forall y (x < y \Rightarrow \neg y < x)$

(O_3) $\forall x \forall y \forall z (x < y \wedge y < z \Rightarrow x < z)$

Ослањајући се на „здраворазумску логику", једноставно уочавамо да се из списка $(*)$ и особина (O_1), (O_2), (O_3) може закључити, на пример: $3 < 6$; $\neg\, 5 < 2$; $\neg\, 7 < 7$ итд.

▼ Задаци и додаци

1. На универзуму људи изабрани су предикати:
   $R(x,y)$ – 'x је родитељ од y';
   $M(x)$ – 'x је мушког пола'.

Саставити формуле:

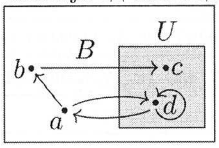
$\varphi_M(x,y)$ – 'x је мајка од y'	$\varphi_B(x,y)$ – 'x и y су рођена браћа'
$\varphi_T(x,y)$ – 'x је тетка од y'	$\varphi_D(x,y)$ – 'x је деда од y'
$\varphi_S(x,y)$ – 'x је стриц од y'	$\varphi_U(x,y)$ – 'x је ујак од y'

2. На универзуму који чине објекти a, b, c, d, e, дефинисана су два предиката: унарни U и бинарни B, следећим таблицама:

x	$U(x)$
a	0
b	0
c	1
d	1

B	a	b	c	d
a	0	1	0	1
b	0	0	1	0
c	0	0	0	0
d	1	0	0	1

Следећи графички приказ универзума и предиката које на њему посматрамо много је упечатљивији од таблица.



а) Одредити истинитосну вредност формуле са једном слободном промењивом x, у зависности од вредности додељене промењивој x.

x	$U(x) \Rightarrow B(x,x)$	$U(x) \vee \neg B(x,x)$	$U(x) \wedge B(x,x)$
a	1		
b	1		
c	0		
d	1		

б) Одредити истинитосну вредност формуле са две слободне промењиве x, y, у зависности од вредности које су додељене промењивама x и y.

x	a	a	a	a	b	b	b	b	c	c	c	c	d	d	d	d
y	a	b	c	d	a	b	c	d	a	b	c	d	a	b	c	d
$U(x) \wedge U(y) \Rightarrow \neg B(x,y)$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
$\neg(U(x) \vee U(y)) \wedge B(x,y)$																
$\neg U(x) \wedge B(x,y) \Rightarrow U(y)$																
$B(x,y) \vee B(y,x)$																
$B(x,y) \vee \neg B(x,y)$																

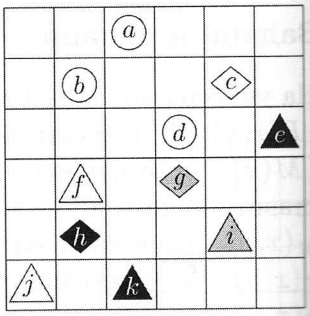
в) Испитати тачност следећих реченица:

- $\exists x (U(x) \Rightarrow B(x,x))$
- $\forall x (B(x,x) \Rightarrow U(x))$
- $\forall x \exists y (B(x,y) \wedge U(y))$
- $\neg \forall x (U(x) \Rightarrow B(x,x))$
- $\forall x \exists y (B(x,y) \wedge U(x))$
- $\forall x (\neg U(x) \Rightarrow \exists y\, (U(y) \wedge B(x,y)))$

3. Да би студентима приближили предикатски језик, логичари Џон Барвајз и Џон Ечеменди креирали су софтвер и написали пратећу књигу *Тарскијев свет*. Универзум Тарскијевог света чине геометријске фигуре, различитих боја, распоређене на квадратној мрежи. Од корисника/читаоца се очекује да састављa предикатске формуле и одреди да ли су тачне или нетачне у датом свету.

Џон Барвајз (1942–2000), амери-чки математичар
Џон Ечеменди (1952–), амерички филозоф

Алфред Тарски (1901–1983) је био пољски математичар који је аутор многих значајних студија из математичке логике.



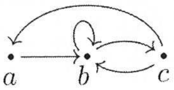
На слици десно приказан је један Тарскијев свет, чији су објекти названи једнословним именима: a, b, c, d, e, f, g, h, i, j, k. Свет се описује следећим предикатима:

$T(x)$ – 'x је троугао' $K(x)$ – 'x је круг' $R(x)$ – 'x је ромб'
$B(x)$ – 'x је бео' $S(x)$ – 'x је сив' $C(x)$ – 'x је црн'
$J(x,y)$ – 'x је јужно од y' (одн. 'x је у реду који је испод y')
$I(x,y)$ – 'x је источно од y' (одн. 'x је у колони која је десно од y')

Попунити табелу:

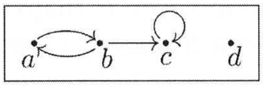
говорни језик	**предикатски језик**	**истинитост**
g је јужно од a	$J(g,a)$	тачно
d није истично од f	$\neg I(d,f)$	нетачно
постоји црни ромб	$\exists x(R(x) \land C(x))$	тачно
сваки круг је бео	$\forall x(K(x) \Rightarrow B(x))$	тачно
постоји троугао источно од a	$\exists x(T(x) \land I(x,a))$	
сваки троугао је јужно од c	$\forall x(T(x) \Rightarrow J(x,c))$	
	$\forall x(T(x) \land J(x,c))$	
	$\exists x(T(x) \land I(a,x))$	
	$\exists x(T(x) \Rightarrow I(a,x))$	
не постоји сиви троугао		
свака црна фигура је ромб или троугао		
сваки црни круг је источно од f		
	$\forall x \forall y(C(x) \land S(y) \Rightarrow I(x,y))$	
	$\exists x(C(x) \land \forall y I(y,x))$	
	$\forall x(B(x) \Rightarrow \exists y I(x,y))$	
	$\exists x(B(x) \land \forall y(C(y) \Rightarrow I(x,y)))$	
	$\forall x(K(x) \lor \exists y J(y,x))$	
постоји ромб и постоји троугао који су исте боје		
постоје сива и црна фигура које су истог облика		

4. Свака формула са једном слободном променљивом $\alpha(x)$ дефинише део универзума који чине само они објекти за које је формула α постаје тачна, када променљиву x заменимо тим објектом. Над универзумом који чине три објекта a, b и c, задат је бинарни предикат: $R(x,y)$ – 'из x иде стрелица ка y'. За сваку од формула $\alpha(x)$ навести за које вредности x је тачна.



$\alpha(x)$	је тачно када x добије вредност:
$\neg R(x,x)$	a, c
$\forall y R(y,x)$	
$\exists y(R(y,x) \wedge R(y,y))$	
$\exists y(R(y,x) \wedge R(x,y))$	
$R(x,x) \Rightarrow \forall y\, R(x,y)$	

5. На универзуму од четири објекта, a, b, c, d, дефинисан је бинарни предикат: $E(x,y)$ – 'из x иде стрелица ка y'



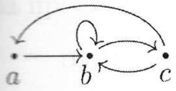
(а) Одредити формулу $\alpha(x)$ која ће бити тачна само када променљива x добије неку од вредности:

- a, b и c (а нетачна је за d);
- a, c и d (а нетачна је за b);
- b и c (а нетачна је за a и d);
- a и b (а нетачна је за c и d).

(б) Испитати тачност следећих реченица:

- $\exists x \forall y \neg E(x,y)$
- $\forall x(E(x,x) \wedge \neg\exists y E(y,x) \Rightarrow \forall z E(x,z))$
- $\forall x(\neg\exists y\, E(x,y) \Rightarrow \neg E(x,x))$
- $\forall x(\exists y\, E(x,y) \Rightarrow \exists z\, E(y,z))$

6. Над универзумом који чине три објекта a, b и c, задат је бинарни предикат R (сликом доле лево, одн. табелом доле десно).



R	a	b	c
a	0	1	0
b	0	1	1
c	1	1	0

(а) Попуњавањем табеле одредити истинитосне вредности формула $\forall y\, R(x,y)$ и $\forall y\, R(y,x)$, за разне вредности слободне променљиве x. (Упутство: за изабрано x, треба за све вредности променљиве y испитати истинитосне вредности формула $R(x,y)$, одн. $R(y,x)$.)

x	y	$R(x,y)$	$\forall y\, R(x,y)$	$R(y,x)$	$\forall y\, R(y,x)$
	a	0			
a	b	1	0		
	c	0			
	a				
b	b				
	c				
	a				
c	b				
	c				

(б) Испитати тачност следећих реченица:

- $\neg\exists x \forall y\, R(x,y)$
- $\exists x \forall y\, R(y,x)$
- $\forall x \exists y\, \neg R(x,y)$
- $\forall y \exists x\, R(y,x)$

Формуле постају разумљивије, ако $R(x,y)$ читамо као реченицу

из x иде стрелица ка y.

Тада:

- $\forall y R(x,y)$ значи *из x иде стрелица ка сваком објекту*;
- $\forall y R(y,x)$ значи *из сваког објекта иде стрелица ка x*;
- $\exists y R(x,y)$ значи *из x иде стрелица ка неком објекту*;
- $\exists y R(y,x)$ значи *постоји објекат из ког иде стрелица ка x*;
- $\exists x \forall y\, R(x,y)$ значи *постоји објекат из ког иде стрелица ка сваком објекту*;
- $\forall x \exists y\, R(x,y)$ значи *из сваког објекта иде стрелица ка неком објекту*;

3.3 Предикатска природна дедукција

Увод. Велику историјску вредност има Аристотелова силогистика која представља први покушај изградње једног формалнологичког система. Разматране су реченице следећег облика:

(aSP) *Сви S јесу P* (универзално афирмативна реченица)
(eSP) *Ниједан S није P* (универзално негативна реченица)
(iSP) *Неки S јесу P* (партикуларно афирмативна реченица)
(oSP) *Неки S нису P* (партикуларно негативна реченица)

Аристотел (384.п.н.е.–322.п.н.е.) се сматра једним од најутицајнијих личности антике.
Од давнина се самогласници a, e, i, o користе за означавање наведених типова реченица.

Са данашњег становишта, Аристотелов систем је само једноставни део предикатске логике унарних предиката, коју разматрамо искључиво на непразним универзумима.

(aSP) *Сви S јесу P*: $\forall x(S(x) \Rightarrow P(x))$
(eSP) *Ниједан S није P*: $\forall x(S(x) \Rightarrow \neg P(x))$
(iSP) *Неки S јесу P*: $\exists x(S(x) \wedge P(x))$
(oSP) *Неки S нису P*: $\exists x(S(x) \wedge \neg P(x))$

Главни проблем који је Аристотел решавао јесте трагање за типом закључка из две хипотезе у којима учествују три предиката (термина, како их је Аристотел звао): мали, велики, средњи. Средњи предикат, заједнички за обе хипотезе, посредовао је у извођењу закључка о малом и великом предикату. Наводимо неколико силогизама:

(ePM)	Ниједан P није M.	(aMP)	Сваки M јесте P.
(iSM)	Неки S јесу M.	(iSM)	Неки S јесу M.
(oSP)	Неки S нису P.	(iSP)	Неки S јесу P.

Као корисну вежбу остављамо да се одреде закључци следећих силогизама.

(aMP)	(aMP)	(ePM)	(aPM)
(aSM)	(iSM)	(aSM)	(oSM)

Наравно, важну улогу у извођењу коректних закључка имају правила која се односе на квантификаторе и која су тема овог одељка. Тим правилима проширујемо исказну природну дедукцију.

План

- правила природне дедукције за квантификаторе: увођење и елиминација квантификатора
- теореме предикатског рачуна: Де Морганови закони за квантификаторе, суседни квантификатори, однос квантификатора и логичких везника

Поред правила дедукције за исказне везнике, која примењујемо и за предикатске формуле, користимо и правила за квантификаторе.

Важно место у правилима дедукције која се односе на квантификаторе заузима тзв. **супституција** слободних променљивих симболима константи или неким другим променљивама.

Ако је α нека формула, x променљива и c симбол константе, онда са $\alpha[x/c]$ означавамо формулу добијену заменом свих слободних појављивања променљиве x симболом константе c. Наравно, ако x није слободно у α, онда је формула $\alpha[x/c]$ истоветна формули α.

Приликом замене слободне променљиве неком другом променљивом неопходно је испоштовати следећи захтев: када у α свако слободно појављивање променљиве x замењујемо променљивом y, ниједно појављивање променљиве y након замене x са y, не сме да постане везано. У наредном примеру, илуструјемо разлоге овог ограничења.

Пример 31. Ако се ослонимо на интерпретацију из уводног примера за претходни одељак, онда се формула

$$\alpha(y) : \forall x\, V(x, y) \text{ – свака особа воли особу } y$$

битно не разликује од формуле

$$\alpha(y)[y/z] : \forall x\, V(x, z) \text{ – свака особа воли особу } z;$$

у оба случаја истинитост добијених формула зависи од вредности које доделимо променљивој y, одн. z. Исто важи ако y заменимо било којом другом променљивом, осим променљивом x, јер би то изазвало драстичну промену значења:

$$\alpha(y)[y/x] : \forall x\, V(x, x) \text{ – свака особа воли себе.}$$

Не постоји нека суштинска разлика да ли квадратну функцију задајемо једнакошћу $f(y) = y^2$ или $f(z) = z^2$.

Кажемо да је променљива x **слободна за** y **у формули** α ако ниједно појављивање променљиве y настало заменом x са y не постаје везано, а са $\alpha[x/y]$ означавамо формулу добијену након описане замене. У наставку, када год напишемо $\alpha[x/y]$ подразумеваћемо да је променљива x слободна за y у формули α. Када је јасно да је у формули α променљива x замењена променљивом y, уместо $\alpha[x/y]$ краће пишемо $\alpha(y)$.

Приметимо да је x увек слободно за x и да је формула $\alpha[x/x]$ истоветна формули α. Такође, уколико се променљива x не појављује слободно у формули α, тада је формула $\alpha[x/y]$ идентична формули α.

Правила $\forall x_{\mathrm{E}}$ и $\exists x_{\mathrm{U}}$

Пре него што наведемо насловљена правила мотивисаћемо их неким интуитивним аргументима. Нека је P унарни предикатски симбол. Ако замислимо да су низом $c_1, c_2, c_3, \ldots$ набројани сви објекти универзума, тада формула $\forall x P(x)$ „тврди”:

(1) $$P(c_1) \wedge P(c_2) \wedge P(c_3) \wedge \cdots ,$$

а $\exists x P(x)$ „тврди":

$$P(c_1) \lor P(c_2) \lor P(c_3) \lor \cdots . \qquad (2)$$

Ова запажања нас наводе да правила дедукције о квантификаторима повежемо са одговарајућим правилима за конјункцију и дисјункцију.

Правило ($\land_E$)

$$\frac{P(c_1) \land P(c_2) \land P(c_3) \land \cdots}{P(c_i)} \ (\land_E)$$

тесно је повезано са следећим размишљањем: ако је тачно $\forall x\alpha$, тада ће бити тачна и формула добијена када се у α променљива x замени било којим објектом.

$$\boxed{\frac{\forall x\alpha}{\alpha[x/v]} \ (\forall_E)}$$

Из $\forall x\alpha$ закључујемо $\alpha[x/v]$, где је v симбол константе или променљива за коју је x слободно у α.

Будући да на располагању имамо неограничено много променљивих, за сваку формулу α можемо пронаћи променљиву v тако да након замене x са v у α, ниједно појављивање променљиве v не постаје везано.

Пример 32.

$\forall x(\texttt{Covek}(x) \Rightarrow \texttt{Smrtan}(x)), \texttt{Covek}(\texttt{Sokrat}) \vdash \texttt{Smrtan}(\texttt{Sokrat})$

1.	$\forall x(\texttt{Covek}(x) \Rightarrow \texttt{Smrtan}(x))$	претпоставка
2.	$\texttt{Covek}(\texttt{Sokrat})$	претпоставка
3.	$\texttt{Covek}(\texttt{Sokrat}) \Rightarrow \texttt{Smrtan}(\texttt{Sokrat})$	$\forall x_E$, 1 $[x/\texttt{Sokrat}]$
4.	$\texttt{Smrtan}(\texttt{Sokrat})$	$\Rightarrow_E$, 3, 2

Правило ($\lor_U$)

$$\frac{R(c_i)}{R(c_1) \lor R(c_2) \lor R(c_3) \lor \cdots} \ (\lor_U)$$

тесно је повезано са следећим размишљањем: ако је тачно $\alpha[x/v]$ за неки објекат v, онда је тачна и формула $\exists x\alpha$.

$$\boxed{\frac{\alpha[x/v]}{\exists x\alpha} \ (\exists_U)}$$

Из $\alpha[x/v]$, за неки симбол константе или променљиву v, закључујемо $\exists x\alpha$.

Пример 33.

$\forall x(\texttt{Covek}(x) \Rightarrow \texttt{Smrtan}(x)), \texttt{Covek}(\texttt{Sokrat}) \vdash \exists x\texttt{Smrtan}(x)$

1.	$\forall x(\texttt{Covek}(x) \Rightarrow \texttt{Smrtan}(x))$	претпоставка
2.	$\texttt{Covek}(\texttt{Sokrat})$	претпоставка
3.	$\texttt{Covek}(\texttt{Sokrat}) \Rightarrow \texttt{Smrtan}(\texttt{Sokrat})$	$\forall x_E$, 1 $[x/\texttt{Sokrat}]$
4.	$\texttt{Smrtan}(\texttt{Sokrat})$	$\Rightarrow_E$, 3, 2
5.	$\exists x\texttt{Smrtan}(x)$	$\exists x_U$, 4

Правила $\forall x_{\mathrm{U}}$ и $\exists x_{\mathrm{E}}$

Увођење универзалног и елиминација егзистенцијалног квантификатора су донекле компликованија правила.

Неформално, када треба да докажемо тврдњу облика $\forall x\alpha$, доказивање започињемо речима „нека је x произвољан објекат ...", при чему водимо рачуна да је једино што знамо о x-у то да припада одговарајућем универзуму; уколико се деси да је ознака x већ искоришћена, онда узимамо неку другу, **свежу** променљиву v и кажемо „нека је v произвољан објекат ..." Слично томе, када знамо да је тачно $\exists x\alpha$, онда ћемо одговарајући елемент означити неким „свежим" словом које није већ резервисано.

У оба правила се појављују поддокази снабдевени тзв. *свежом променљивом* која се у формулама ван поддоказа не појављује слободно.

$$\frac{\begin{array}{l} v \\ \vdots \\ \alpha[x/v] \end{array}}{\forall x\alpha}\ (\forall x_{\mathrm{U}})$$

Ако се коришћењем *свеже* променљиве може доказати $\alpha[x/v]$, онда се може закључити $\forall x\alpha$.

Кључна чињеница за претходно правило јесте да је v свежа променљива, тј. да се не појављује нигде ван одговарајућег поддоказа, па пошто ништа не претпостављамо о v, сваки објекат „пролази" на његовом месту. Следећа шема илуструје употребу правила $(\forall x_{\mathrm{U}})$.

⋮			Када желимо да докажемо $\forall x\alpha$,
j.	v		уводимо свежу променљиву v, размишљајући „нека је v произвољан објекат универзума".
⋮	⋮		Из свега осталог настојимо да докажемо $\alpha[x/v]$.
k.	$\alpha[x/v]$		Када успемо,
$k+1$.	$\forall x\alpha$	$(\forall x_{\mathrm{U}})$, j-k	изводимо жељени закључак.

Пример 34. Докажимо секвент
$\forall x(A(x) \Rightarrow B(x)), \forall x(B(x) \Rightarrow C(x)) \vdash \forall x(A(x) \Rightarrow C(x))$.

1.	$\forall x(A(x) \Rightarrow B(x))$	претпоставка
2.	$\forall x(B(x) \Rightarrow C(x))$	претпоставка
3.	v	уводимо свежу променљиву
4.	$A(v) \Rightarrow B(v)$	$\forall x_{\mathrm{E}}$, 1
5.	$B(v) \Rightarrow C(v)$	$\forall x_{\mathrm{E}}$, 2
6.	$A(v) \Rightarrow C(v)$	транзитивност импликације, 4, 5
7.	$\forall x(A(x) \Rightarrow C(x))$	$\forall x_{\mathrm{U}}$, 3-6

Уведимо најзад правило $(\exists x_{\mathrm{E}})$. Грубо речено: ако знамо да је $\exists x\alpha$ тачно, онда је α тачно за бар једну вредност x, па би требало

обавити закључивање по случајевима за све могуће вредности, што постижемо користећи свежу променљиву v као генеричку вредност која репрезентује све могуће вредности.

$$\dfrac{\exists x\alpha \qquad \begin{array}{|ll} v & \alpha[x/v] \\ & \vdots \\ & \gamma \end{array}}{\gamma}\ (\exists x_{\mathrm{E}})$$

Ако из $\alpha[x/v]$ докажемо формулу γ у којој се не појављује v, онда γ мора бити тачно без обзира на вредност v. И овога пута, од суштинске важности је да се v не појављује слободно нигде ван одговарајућег поддоказа, па самим тим ни у γ.

Следећа шема илуструје коришћење правила ($\exists x_{\mathrm{E}}$).

$\vdots$			
$i.$	$\exists x\alpha$		
$\vdots$			Када желимо да искористимо $\exists x\alpha$,
$j.$	$\vert\ v\ \ \alpha[x/v]$	дод. прет.	уводимо ознаку v за објекат који задовољава α.
$\vdots$	$\vert\ \ \vdots$		Из $\alpha[x/v]$ и свега осталог настојимо да докажемо γ у коме се v не појављује слободно.
$k.$	$\vert\ \ \gamma$		Када успемо,
$k+1.$	γ	$(\exists x_{\mathrm{E}})$, i, j-k	изводимо жељени закључак.

Пример 35. Докажимо секвент:

$$\exists x(D(x) \land \forall y(M(y) \Rightarrow V(y,x))), M(c) \vdash \exists z V(c,z)$$

1.	$\exists x(D(x) \land \forall y(M(y) \Rightarrow V(y,x)))$	претпоставка
2.	$M(c)$	претпоставка
3.	$\vert\ d\ \ D(d) \land \forall y(M(y) \Rightarrow V(y,d))$	додатна претпоставка
4.	$\vert\ \ \ \forall y(M(y) \Rightarrow V(y,d))$	$\land^{\mathrm{D}}_{\mathrm{E}}$, 3
5.	$\vert\ \ \ M(c) \Rightarrow V(c,d)$	$\forall y_{\mathrm{E}}$, 4 (применом $[y/c]$)
6.	$\vert\ \ \ V(c,d)$	$\Rightarrow_{\mathrm{E}}$, 5, 2
7.	$\vert\ \ \ \exists z V(c,z)$	$\exists z_{\mathrm{U}}$, 6
8.	$\exists z V(c,z)$	$\exists x_{\mathrm{E}}$, 1, 3-7

Формула α је **теорема предикатског рачуна** ако је доказив секвент $\vdash \alpha$. Наводимо неколико важних теорема предикатског рачуна који се често могу препознати у математичким доказима.

Два суседна квантификатора исте врсте могу заменити места.
$\vdash \forall x\forall y\alpha \Leftrightarrow \forall y\forall x\alpha \quad \vdash \exists x\exists y\alpha \Leftrightarrow \exists y\exists x\alpha$

$\vdash \exists x\forall y\alpha \Rightarrow \forall y\exists x\alpha$

Доказе претходних секвената остављамо за вежбу.

Де Морганови закони за квантификаторе:
$\vdash \neg\exists x\alpha \Leftrightarrow \forall x\neg\alpha \quad \vdash \neg\forall x\alpha \Leftrightarrow \exists x\neg\alpha$

Докажимо Де Морганов закон $\vdash \neg\exists x\alpha \Leftrightarrow \forall x\neg\alpha$. Наводимо [illegible] доказе секвената $\neg\exists x\alpha \vdash \forall x\neg\alpha$ и $\forall x\neg\alpha \vdash \neg\exists x\alpha$.

Де Морганови закон $\vdash \neg\exists x\alpha \Leftrightarrow \forall x\neg\alpha$

1.	$\neg\exists x\alpha$	претпоставка	1.		$\forall x\neg\alpha$	претпоставка
2.	v		2.		$\exists x\alpha$	додатна прет.
3.	$\alpha[x/v]$	додатна прет.	3.	v	$\alpha[x/v]$	додатна прет.
4.	$\exists x\alpha$	$\exists x_{\mathrm{U}}$, 3	4.		$\neg\alpha[x/v]$	$\forall x_{\mathrm{E}}$, 1
5.	$\bot$	$\neg_{\mathrm{E}}$, 4, 1	5.		$\bot$	$\neg_{\mathrm{E}}$, 3, 4
6.	$\neg\alpha[x/v]$	$\neg_{\mathrm{U}}$, 3-5	6.	$\bot$		$\exists x_{\mathrm{E}}$, 2, 3-5
7.	$\forall x\neg\alpha$	$\forall x_{\mathrm{U}}$, 2-6	7.		$\neg\exists x\alpha$	$\neg_{\mathrm{U}}$, 2-6

Де Морганов закон $\vdash \neg\forall x\alpha \Leftrightarrow \exists x\neg\alpha$ једноставно изводимо из претходног. Доказ наводимо у облику еквиваленцијског ланца:

$$\neg\forall x\alpha \Leftrightarrow \neg\forall x\neg\neg\alpha \Leftrightarrow \neg\neg\exists x\neg\alpha \Leftrightarrow \exists x\neg\alpha$$

$\forall$ пролази кроз $\wedge$, а $\exists$ кроз $\vee$:
$\vdash \forall x(\alpha\wedge\beta) \Leftrightarrow \forall x\alpha \wedge \forall x\beta \quad \vdash \exists x(\alpha\vee\beta) \Leftrightarrow \exists x\alpha \vee \exists x\beta$

$\vdash \forall x\alpha \vee \forall x\beta \Rightarrow \forall x(\alpha\vee\beta) \quad \vdash \exists x(\alpha\wedge\beta) \Rightarrow \exists x\alpha \wedge \exists x\beta$

Да бисмо доказали да $\forall$ пролази кроз $\wedge$ доказаћемо секвенте $\forall x(\alpha\wedge\beta) \vdash \forall x\alpha \wedge \forall x\beta$ и $\forall x\alpha \wedge \forall x\beta \vdash \forall x(\alpha\wedge\beta)$.

Доказ за $\forall x(\alpha\wedge\beta) \vdash \forall x\alpha \wedge \forall x\beta$

1.		$\forall x(\alpha\wedge\beta)$	претпоставка
2.	x		Докажимо најпре $\forall x\alpha$.
3.		$\alpha\wedge\beta$	$\forall x_{\mathrm{E}}$, 1
4.		α	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 3
5.		$\forall x\alpha$	$\forall x_{\mathrm{U}}$, 2-4
6.	x		Докажимо даље $\forall x\beta$.
7.		$\alpha\wedge\beta$	$\forall x_{\mathrm{E}}$, 1
8.		β	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 7
9.		$\forall x\beta$	$\forall x_{\mathrm{U}}$, 6-8
10.		$\forall x\alpha \wedge \forall x\beta$	$\wedge_{\mathrm{U}}$, 5, 9

Доказ за $\forall x\alpha \wedge \forall x\beta \vdash \forall x(\alpha\wedge\beta)$

1.		$\forall x\alpha \wedge \forall x\beta$	претпоставка
2.		$\forall x\alpha$	$\wedge^{\mathrm{L}}_{\mathrm{E}}$, 1
3.		$\forall x\beta$	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 1
4.	x		
5.		α	$\forall x_{\mathrm{E}}$, 2
6.		β	$\forall x_{\mathrm{E}}$, 3
7.		$\alpha\wedge\beta$	$\wedge_{\mathrm{U}}$, 5, 6
8.		$\forall x(\alpha\wedge\beta)$	$\forall x_{\mathrm{U}}$, 4-7

Доказ да $\exists$ пролази кроз $\vee$ наводимо у облику еквиваленцијског ланца.

$$\begin{aligned}
\exists x(\alpha\vee\beta) &\Leftrightarrow \neg\neg\exists x(\alpha\vee\beta)\\
&\Leftrightarrow \neg\forall x\neg(\alpha\vee\beta)\\
&\Leftrightarrow \neg\forall x(\neg\alpha\wedge\neg\beta)\\
&\Leftrightarrow \neg(\forall x\neg\alpha\wedge\forall x\neg\beta)\\
&\Leftrightarrow \neg\forall x\neg\alpha\vee\neg\forall x\neg\beta\\
&\Leftrightarrow \exists x\neg\neg\alpha\vee\exists x\neg\neg\beta\\
&\Leftrightarrow \exists x\alpha\vee\exists x\beta
\end{aligned}$$

Ако x нема слободно појављивање у β:
$\vdash \forall x(\alpha \lor \beta) \Leftrightarrow \forall x\alpha \lor \beta$ $\qquad \vdash \exists x(\alpha \land \beta) \Leftrightarrow \exists x\alpha \land \beta$
Ако x нема слободно појављивање у β:
$\vdash \forall x(\alpha \Rightarrow \beta) \Leftrightarrow (\exists x\alpha \Rightarrow \beta)$ $\quad \vdash \exists x(\alpha \Rightarrow \beta) \Leftrightarrow (\forall x\alpha \Rightarrow \beta)$

Под претпоставком да x нема слободно појављивање у β, доказаћемо $\exists x(\alpha \land \beta) \vdash \exists x\alpha \land \beta$ и $\exists x\alpha \land \beta \vdash \exists x(\alpha \land \beta)$.

Доказ за $\exists x(\alpha \land \beta) \vdash \exists x\alpha \land \beta$, када x није слободно у β.

1.	$\exists x(\alpha \land \beta)$	претпоставка
2	$\mid v \;\; \alpha[x/v] \land \beta$	додатна прет. ($\beta[x/v]$ је истоветно формули β)
3.	$\mid \;\; \alpha[x/v]$	$\land_{\mathrm{E}}^{\mathrm{L}}$, 2
4.	$\mid \;\; \beta$	$\land_{\mathrm{E}}^{\mathrm{D}}$, 3
5.	$\mid \;\; \exists x\alpha$	$\exists x_{\mathrm{U}}$, 3
6.	$\mid \;\; \exists x\alpha \land \beta$	$\land_{\mathrm{U}}$, 5, 4
7.	$\exists x\alpha \land \beta$	$\exists x_{\mathrm{E}}$, 1, 2-6

Доказ за $\exists x\alpha \land \beta \vdash \exists x(\alpha \land \beta)$, када x није слободно у β.

1.	$\exists x\alpha \land \beta$	претпоставка
2.	$\exists x\alpha$	$\land_{\mathrm{E}}^{\mathrm{L}}$, 1
3.	β	$\land_{\mathrm{E}}^{\mathrm{D}}$, 1
4	$\mid v \;\; \alpha[x/v]$	додатна прет.
5.	$\mid \;\; \alpha[x/v] \land \beta$	$\land_{\mathrm{U}}$, 4, 3
6.	$\mid \;\; \exists x(\alpha \land \beta)$	$\land_{\mathrm{E}}^{\mathrm{D}}$, 5 ($\beta[x/v]$ је истоветно формули β)
7.	$\exists x(\alpha \land \beta)$	$\exists x_{\mathrm{E}}$, 2, 4-6

Доказе последња два секвента остављамо за вежбу.

Одељак завршавамо примером који показује однос између извођења у природној дедукцији и доказивања које се обично наводи у математици.

Пример 36. Нека универзум чине све тачке неке равни. Да бисмо описали распоред међу тачкама користићемо тернарни (дужине три) предикатски симбол O: $O(x, y, z)$ значи „тачка y је између тачака x и z". Доказати да из „очигледне истине", тј. аксиоме[87]:
$\forall x \forall y \forall z(O(x, y, z) \Rightarrow O(z, y, x) \land \neg O(y, z, x))$
следи $\forall x \forall y \forall z(O(x, y, z) \Rightarrow \neg O(z, x, y))$.
'Обичан' математички доказ:

Претпоставимо $\forall x \forall y \forall z(O(x, y, z) \Rightarrow O(z, y, x) \land \neg O(y, z, x))$ $(*)$

Нека су a, b, c произвољне тачке.

Да бисмо доказали импликацију $O(a, b, c) \Rightarrow \neg O(c, a, b)$,

претпоставимо да је $O(a, b, c)$. (Треба доказати $\neg O(c, a, b)$.)

Претпоставимо (супротно), да је $O(c, a, b)$.

Из $(*)$ и $O(c, a, b)$ следи $O(b, a, c)$ и $\neg O(a, b, c)$

(На $(*)$ смо применили $[x/c], [y/b], [z/a]$.)

$O(a, b, c)$ и $\neg O(a, b, c)$ дају контрадикцију.

Дакле, $\neg O(c, a, b)$.

[87] Ако је тачка y између x и z, онда је y између z и x, и z није између y и z.

Дакле, $O(a,b,c) \Rightarrow \neg O(c,a,b)$.

Дакле, $\forall x \forall y \forall z (O(x,y,z) \Rightarrow \neg O(z,x,y))$.

Доказ природном дедукцијом:

1.	$\forall x \forall y \forall z (O(x,y,z) \Rightarrow O(z,y,x) \wedge \neg O(y,z,x))$	претпоставка
2.	a, b, c	
3.	$O(a,b,c)$	додатна претпоставка
4.	$O(c,a,b)$	додатна претпоставка
5.	$O(c,a,b) \Rightarrow O(b,a,c) \wedge \neg O(a,b,c)$	$\forall xyz_{\mathrm{E}}$, 1
6.	$O(b,a,c) \wedge \neg O(a,b,c)$	$\Rightarrow_{\mathrm{E}}$, 5, 4
7.	$\neg O(a,b,c)$	$\wedge^{\mathrm{D}}_{\mathrm{E}}$, 6
8.	$\bot$	$\neg_{\mathrm{E}}$, 3, 7
9.	$\neg O(c,a,b)$	$\neg_{\mathrm{U}}$, 4-8
10.	$O(a,b,c) \Rightarrow \neg O(c,a,b)$	$\Rightarrow_{\mathrm{U}}$, 3-9
11.	$\forall x \forall y \forall z (O(x,y,z) \Rightarrow \neg O(z,x,y))$	$\forall xyz_{\mathrm{U}}$, 2-10

Задаци и додаци

1. Доказати

а) $\forall x(\texttt{Kos}(x) \Rightarrow \texttt{Ptica}(x)), \neg\texttt{Ptica}(\texttt{Dambo}) \vdash \neg\texttt{Kos}(\texttt{Dambo})$

б) $\forall x(\texttt{Macka}(x) \Rightarrow \texttt{Lovac}(x)), \forall x(\texttt{Lav}(x) \Rightarrow \texttt{Macka}(x)) \vdash \forall x(\neg\texttt{Lovac}(x) \Rightarrow \neg\texttt{Lav}(x))$

в) $\forall x(\texttt{Kelt}(x) \Rightarrow \neg\texttt{Got}(x)), \forall x(\texttt{Gal}(x) \Rightarrow \texttt{Kelt}(x)) \vdash \forall x(\texttt{Got}(x) \Rightarrow \neg\texttt{Gal}(x))$

2. Доказати секвенте:

а) $\vdash \forall x(A(x) \Rightarrow A(x))$

б) $\forall x(A(x) \Rightarrow B(x)), \forall x(B(x) \Rightarrow A(x)) \vdash \forall x(A(x) \Leftrightarrow B(x))$

в) $\vdash \forall x(A(x) \Leftrightarrow A(x))$

г) $\forall x(A(x) \Leftrightarrow B(x)) \vdash \forall x(B(x) \Leftrightarrow A(x))$

д) $\forall x(A(x) \Leftrightarrow B(x)), \forall x(B(x) \Leftrightarrow C(x)) \vdash \forall x(A(x) \Leftrightarrow C(x))$

ђ) $\forall x \neg P(x) \vdash \forall x(P(x) \Rightarrow A(x))$

е) $\forall x \neg P_1(x), \forall x \neg P_2(x) \vdash \forall x(P_1(x) \Leftrightarrow P_2(x))$

3. Доказати:

а) $\forall x(A(x) \Rightarrow B(x)), \exists x \neg B(x) \vdash \exists x \neg A(x)$

б) $\forall x(A(x) \vee B(x) \Rightarrow C(x)), \exists x \neg C(x) \vdash \exists x \neg A(x)$

в) $\forall x(C(x) \Rightarrow A(x)), \forall x(\neg B(x) \Rightarrow C(x)) \vdash \forall x(A(x) \vee B(x))$

г) $\forall x(N(x) \wedge S(x) \Rightarrow C(x)), \forall x(T(x) \Rightarrow N(x)), \exists x(T(x) \wedge \neg C(x)) \vdash \exists x \neg S(x)$

д) $\forall x(N(x) \Rightarrow B(x)), \exists x(N(x) \wedge D(x)) \vdash \exists x(B(x) \wedge D(x))$

ђ) $\forall x((A(x) \Rightarrow R(x)) \vee T(x)), \exists x(T(x) \Rightarrow P(x)), \forall x(A(x) \wedge \neg P(x)) \vdash \exists x R(x)$

е) $\forall x \exists y(E(x) \Rightarrow M(x) \vee N(y)), \neg \forall x M(x), \forall x E(x) \vdash \exists x N(x)$

ж) $\forall x \exists y\,(P(x) \Rightarrow P(y))$

з) $\exists x \forall y(M(x) \wedge (D(y) \Rightarrow V(x,y))), \forall x \forall y(\neg M(x) \vee \neg V(x,y)) \vdash \forall x \neg D(x)$

и) $\forall x(A(x) \Rightarrow B(x)) \vdash \forall x(\exists y(A(y) \wedge C(x,y)) \Rightarrow \exists y(B(x) \wedge C(x,y)))$

ј) $\exists x(F(x) \wedge \forall y(G(y) \Rightarrow H(x,y))), \forall x(F(x) \Rightarrow \forall y(B(y) \Rightarrow \neg H(x,y))) \vdash \forall x(G(x) \Rightarrow \neg B(x))$

к) $\exists x \exists y(A(x) \wedge A(y) \wedge \neg R(x,y)), \forall x \forall y(B(x) \wedge B(y) \Rightarrow R(x,y)) \vdash \exists x(A(x) \wedge \neg B(x))$

л) $\exists x A(x), \forall y\,(A(y) \Rightarrow \exists z\, B(y,z)), \forall x \forall y\,(B(x,y) \Rightarrow B(y,x)) \vdash \exists x \exists y\,(B(x,y) \wedge A(y))$

љ) $\forall x \forall y\,(B(x,y) \Rightarrow B(y,x) \vee B(y,y)), \forall u\,(\exists v\, B(u,v) \Rightarrow C(u)), \forall w \exists z\, B(z,w) \vdash \forall z\, C(z)$

4. Нека је R бинарни предикатски симбол. Доказати секвенте:

а) $\forall x B(x,x) \vdash \forall x \exists y B(x,y)$

(б) $\forall x \forall y (R(x,y) \Rightarrow \neg R(y,x)) \vdash \forall x \neg R(x,x)$

(в) $\forall x \neg R(x,x), \forall x \forall y \forall z (R(x,y) \wedge R(y,z) \Rightarrow R(x,z)) \vdash \forall x \forall y (R(x,y) \Rightarrow \neg R(y,x))$

(г) $\forall x \forall y \forall z (R(x,y) \wedge R(y,z) \Rightarrow \neg R(x,z)) \vdash \forall x \neg R(x,x)$

(д) $\forall x \exists y R(x,y), \forall x \forall y (R(x,y) \Rightarrow R(y,x)), \forall x \forall y \forall z (R(x,y) \wedge R(y,z) \Rightarrow R(x,z)) \vdash \forall x R(x,x)$

5. Из претпоставки

$\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_2,x_3,x_4,x_1))$

$\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_3,x_1,x_2,x_4))$

извести сваку од следећих формула:

- $\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_3,x_4,x_1,x_2))$
- $\forall x_1 \forall x_2 \forall x_3 \forall x_4 (P(x_1,x_2,x_3,x_4) \Rightarrow P(x_4,x_1,x_2,x_3))$

6. Доказати да из

(1) $\forall x \exists y V(x,y)$

(2) $\forall x \forall y \forall u \forall v (V(x,u) \wedge V(y,v) \Rightarrow V(u,v) \vee V(v,u))$

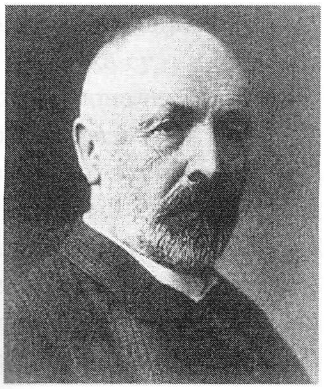
(3) $\forall x \forall y \forall z (V(x,y) \wedge V(y,z) \Rightarrow V(x,z))$

следи $\forall x \forall y \exists z (V(x,z) \wedge V(y,z))$.

3. Теорија скупова **ZF**

Теорија скупова, коју је створио Георг Кантор, [...] изгледа ми као најдивнији плод математичког ума, као једно од највиших достигнућа чисто рационалне људске активности.

Д. Хилберт, цитат из чланка *О бесконачном* (Über das Unendliche), objavljenog 1926. godine



Георг Кантор (1845–1918) био је немачки математичар и зачетник теорије скупова. Настанак теорије скупова се везује за Канторов доказ (из 1873. године) да не постоји функција из скупа природних бројева **на** скуп реалних бројева, и Канторову интерпретацију тог резултата.

3.1. Аксиоме изградње скупова

Увод. Теорија скупова представља заједнички оквир који обједињује различите области математике: алгебру, геометрију, анализу итд. Настаје почетком 20. века, са главним циљем да аксиоматизује интуитивну идеју о *окупљању некаквих објеката у посебну целину*. Окупљене објекте називамо *елементима*, а формирану целину *скуп*. Однос између елемента и скупа означавамо посебним знаком $\in$ и називамо га *припадање*. Потпуно је неважна врста објеката које окупљамо, што значи да и саме скупове можемо окупљати у целине и формирати нове скупове; у оваквим случајевима, припадање је однос између два скупа. Ако се ограничимо само на скупове чији су елементи такође скупови, замишљени универзум скупова можемо описивати користећи предикатски језик са два бинарна предиката $\in$ (припадање) и $=$ (једнакост). Идеју да је скуп одређен само својим елементима изражавамо реченицом: *два скупа су једнака ако имају исте елементе*, тј.
(АКСИОМА ЈЕДНАКОСТИ) $\forall a \forall b (a = b \Leftrightarrow \forall x (x \in a \Leftrightarrow x \in b))$

Почетке проучавања теорије скупова често је пратило наивно прихватање појединих аксиома, које су изгледале интуитивно јасне, али се касније испостављало да доводе до противречности. Најпознатија „наивна аксиома” јесте: за свако својство постоји скуп који садржи само оне објекте који имају то својство.[88] Формулу $\alpha(x, \cdots)$ можемо сматрати својством скупа x, допуштајући могућност да α садржи неке друге променљиве (наведене уместо тачкица $\cdots$). Ако се променљива y не појављује слободно у $\alpha(x, \cdots)$, онда би се „наивна аксиома” могла формулисати овако:
(НАИВНА АКСИОМА!) $\forall \cdots \exists y \forall x (x \in y \Leftrightarrow \alpha(x, \cdots))$
Неприхватљивост „наивна аксиома” показао је Расел изабравши својство *не бити сам себи елемент*, тј. бирајући да $\alpha(x)$ буде $x \notin x$. Из одговарајуће варијанте „наивна аксиома” $\exists y \forall x (x \in y \Leftrightarrow x \notin x)$ изводимо контрадикцију:

1.	$\exists y \forall x (x \in y \Leftrightarrow x \notin x)$	
2.	$\mid\ v\ \ \forall x (x \in v \Leftrightarrow x \notin x)$	
3.	$\mid\ \ v \in v \Leftrightarrow v \notin v$	$\forall x_{\mathrm{E}}$, 2
	$\mid\ \ \vdots$	
$i.$	$\mid\ \ \bot$	
$i+1.$	$\bot$	$\exists x_{\mathrm{E}}$, 1, 2-i

Дакле, „наивна аксиома” је неприхватљива.

План
- језик теорије скупова
- аксиома екстензионалности; основне особине једнакости
- инклузија; основне особине инклузије
- аксиома празног скупа, пара, аксиома уније, аксиома партитивног скупа, схема издвајања
- празан скуп, пар скупова, унија скупа, партитивни скуп скупа, издвајање подскупа

---

[88] „Наивна аксиома” је требало да опише основни начин формирања скупова – *окупљање у целину задавањем својства*, и сходно томе употребу одговарајуће ознаке $\{x \mid \alpha(x, \cdots)\}$ за скуп свих објеката x који имају својство $\alpha(x, \cdots)$.

Бертран Расел (1872–1970), енглески филозоф

Универзум скупова описујемо користећи два бинарна предиката $\in$ (припадање) и $=$ (једнакост). Променљиве ћемо означавати малим и великим словима латинице са индексима или без њих. Уместо $\in(\cdot,\cdot)$ и $=(\cdot,\cdot)$ користићемо тзв. инфиксну нотацију $\cdot \in \cdot$ и $\cdot = \cdot$. За негације атомских формула користимо краће ознаке: уместо $\neg x \in y$ и $\neg x = y$ редом пишемо $x \notin y$ и $x \neq y$.

Основна, унапред претпостављена својства универзума називамо *аксиомама теорије скупова*. Све дедуктивне последице које изводимо из аксиома називамо *теоремама теорије скупова*. При доказивању теорема, полазимо од аксиома и већ доказаних теорема и примењујемо уведена правила дедукције заједно са следећим правилом које се односи на знак $=$:

$$\frac{\varphi[x/u] \qquad u = v}{\varphi[x/v]} \ (=_{\mathrm{E}}).$$

Иако су аксиоме и теореме заправо формуле изабраног предикатског језика, ми ћемо их формулисати и на говорном (српском) језику, јер то значајно олакшава разумевање онога што се њима тврди.

Прва аксиома коју наводимо описује везу између $\in$ и $=$.

Аксиома екстензионалности. Два скупа су једнака ако и само ако имају исте елементе.

$$\forall a \forall b (a = b \Leftrightarrow \forall x (x \in a \Leftrightarrow x \in b))$$

Најпре доказујемо неке очекиване особине једнакости.

Теорема 11. *(1) За сваки скуп a важи $a = a$.*
(2) За све скупове a и b, из $a = b$ следи $b = a$.
(3) За све скупове a, b, c, из $a = b$ и $b = c$ следи $a = c$.

Доказ. Формалне доказе, применом правила природне дедукције, остављамо за вежбу (видети задатак 2, на страни 83). Овде наводимо само кратке коментаре.

(1) Нека је a произвољан скуп. Једноставно се може доказати формула $\forall x(x \in a \Leftrightarrow x \in a)$, из које према аксиоми екстензионалности добијамо $a = a$.

(2) Нека су a и b произвољни скупови. Из $a = b$, према аксиоми екстензионалности следи $\forall x(x \in a \Leftrightarrow x \in b)$, одакле се једноставно може извести $\forall x(x \in b \Leftrightarrow x \in a)$. Из последње формуле, према наведеној аксиоми, добијамо $b = a$.

(3) Нека су a, b и c произвољни скупови. Претпоставимо да важи $a = b$ и $b = c$. Према аксиоми екстензионалности имамо $\forall x(x \in a \Leftrightarrow x \in b)$ и $\forall x(x \in b \Leftrightarrow x \in c)$, одакле изводимо $\forall x(x \in a \Leftrightarrow x \in c)$. Најзад, из последње формуле, применом аксиоме екстензионалности, добијамо $a = c$. □

Неформално, уколико су сви елементи скупа a уједно и елементи скупа b, кажемо да је a *подскуп* од b и пишемо $a \subseteq b$:

$a \subseteq b$ је скраћени запис формуле $\forall x(x \in a \Rightarrow x \in b)$.

Однос међу скуповима означен симболом $\subseteq$ назива се **инклузија**.

Теорема 12. *(1) За сваки скуп a важи $a \subseteq a$.*
(2) За све скупове a и b, из $a \subseteq b$ и $b \subseteq a$ следи $a = b$.
(3) За све скупове a, b, c, из $a \subseteq b$ и $b \subseteq c$ следи $a \subseteq c$.

Доказ. Следеће секвенте није тешко доказати (докази су потпуно аналогни доказима секвената из задатка 2, на страни 83):
(1) $\forall x(x \in a \Rightarrow x \in a)$
(2) $\forall x(x \in a \Rightarrow x \in b), \forall x(x \in b \Rightarrow x \in a) \vdash \forall x(x \in a \Leftrightarrow x \in b)$
(3) $\forall x(x \in a \Rightarrow x \in b), \forall x(x \in b \Rightarrow x \in c) \vdash \forall x(x \in a \Rightarrow x \in c)$
одакле непосредно (уз примену аксиоме екстензионалности за (2)) следе тврђења наведена у леми. □

Преостале аксиоме које наводимо у овом делу су облика

$$(*) \qquad \forall \cdots \exists y \forall x(x \in y \Leftrightarrow \alpha(x, \cdots)),$$

где је $\alpha(x, \cdots)$ формула која поред променљиве x, може да садржи и неке друге променљиве (наведене уместо тачкица $\cdots$), при чему се y не појављује слободно у $\alpha(x, \cdots)$. Формулу $(*)$ схватамо на следећи начин: за произвољне скупове $\cdots$, постоји скуп y који садржи само оне x за које се може утврдити веза $\alpha(x, \cdots)$. Из аксиоме екстензионалности, скуп y чије се постојање тврди формулом $(*)$ мора бити јединствен. Другим речима, из претпоставки

$$\forall x(x \in y_1 \Leftrightarrow \alpha(x, \cdots)) \text{ и } \forall x(x \in y_2 \Leftrightarrow \alpha(x, \cdots)),$$

при чему се y_1 и y_2 не појављују слободно у $\alpha(x, \cdots)$, једноставно се доказује: $\forall x(x \in y_1 \Leftrightarrow x \in y_2)$, одакле, користећи аксиому екстензионалности добијамо $y_1 = y_2$.

Уопште, формуле облика

$$\exists y \varphi(y) \wedge \forall y_1 \forall y_2(\varphi[y/y_1] \wedge \varphi[y/y_2] \Rightarrow y_1 = y_2),$$

које краће означавамо $\exists! y \varphi(y)$, тврде да постоји јединствени објекат y који задовољава извесну формулу φ.

Изводимо важан закључак из претходних разматрања:

$$\frac{\forall a \forall b(a = b \Leftrightarrow \forall x(x \in a \Leftrightarrow x \in b)) \quad \forall \cdots \exists y \forall x(x \in y \Leftrightarrow \alpha(x, \cdots))}{\forall \cdots \exists! y \forall x(x \in y \Leftrightarrow \alpha(x, \cdots))}$$

Овај закључак ћемо применити за сваку од аксиома које наводимо у наставку.

Аксиома празног скупа. Постоји скуп који нема елемената.

$$\exists y \forall x(x \in y \Leftrightarrow \bot).$$

Приметимо да се аксиома може формулисати и на следећи начин: $\exists y \forall x(x \notin y)$ Јединствени скуп који нема елемената означавамо $\emptyset$ и називамо *празан скуп*. Дакле, $\forall x\,(x \notin \emptyset)$. У наставку, ознаку $\emptyset$ користимо као симбол *константе* универзума скупова.

Аксиома пара. За свака два скупа a_1 и a_2 постоји скуп y чији су једини елементи a_1 и a_2.

$$\forall a_1 \forall a_2 \exists y \forall x (x \in y \Leftrightarrow x = a_1 \vee x = a_2)$$

Пошто се може доказати $\forall a_1 \forall a_2 \exists ! y \forall x (x \in y \Leftrightarrow x = a_1 \vee x = a_2)$, јединствени скуп који садржи a_1 и a_2, као једине елементе, означавамо $\{a_1, a_2\}$. Специјално, за произвољан a_1, скуп $\{a_1, a_1\}$ означавамо $\{a_1\}$ и називамо га *синглтон* (или једночлани скуп). Уведене ознаке користимо при записивању формула, имајући на уму да ове ознаке можемо елиминисати помоћу следећих еквиваленција:

$$x \in \{a_1, a_2\} \Leftrightarrow x = a_1 \vee x = a_2 \ \text{ и } \ x \in \{a_1\} \Leftrightarrow x = a_1 \vee x = a_1 \Leftrightarrow x = a_1.$$

Аксиома уније. За сваки скуп a постоји скуп који садржи све елементе елемената скупа a и других елемената нема:

$$\forall a \exists y \forall x (x \in y \Leftrightarrow \exists t (t \in a \wedge x \in t))$$

Јединствени скуп, чије постојање тврди аксиома уније, означавамо $\bigcup a$ или $\bigcup\limits_{t \in a} t$ и називамо *унијом* скупа a.

$$x \in \bigcup a \Leftrightarrow \exists t (t \in a \wedge x \in t)$$

Корисно је имати на уму следеће:

- на пример, ако $\{a, b, c\} \in X$, онда $a, b, c \in \bigcup X$;
- на пример, ако $a, b, c \in X$, онда $\{a, b, c\} \in \mathcal{P}(X)$.

Аксиома партитивног скупа. За сваки скуп a постоји скуп који садржи све подскупове скупа a и других елемената нема:

$$\forall a \exists y \forall x (x \in y \Leftrightarrow \forall t (t \in x \Rightarrow t \in a)), \text{ тј. } \forall a \exists y \forall x (x \in y \Leftrightarrow x \subseteq a)$$

Јединствени скуп, чије постојање тврди аксиома партитивног скупа означавамо $\mathcal{P}(a)$ и називамо *партитивни скуп* од a. Посебно истичемо еквиваленцију коју користимо при раду са партитивним скуповима: $x \in \mathcal{P}(a) \Leftrightarrow x \subseteq a$.

Схема издвајања. За произвољне скупове $a, a_1, \dots, a_n$ и формулу (својство) $\varphi(x, a, a_1, \dots, a_n)$ постоји скуп y који садржи само оне елементе x из a за које важи $\varphi(x, a, a_1, \dots, a_n)$:

$$\forall a \forall a_1 \cdots \forall a_n \exists y \forall x (x \in y \Leftrightarrow x \in a \wedge \varphi(x, a, a_1, \dots, a_n))$$

Да бисмо једноставније објаснили значење аксиоме издвајања, посматраћемо њен специјалан случај

$$\forall a \exists y \forall x (x \in y \Leftrightarrow x \in a \wedge \varphi(x, a)).$$

Схема издвајања заправо одређује бесконачно много аксиома – по једну аксиому, за сваку формулу $\varphi(x, \cdots)$. Уопштено говорећи, за свако задато својство $\varphi(x, \cdots)$, само из постојећих скупова могу се издвајати елементи који задовољавају то својство и од тих елемената формирати нови скуп.

$$\{x \in a \mid \varphi(x, \cdots)\}$$

Овим обликом аксиоме се тврди да за сваки скуп a и било коју формулу $\varphi(x, a)$ можемо формирати скуп (издвојити подскуп од a) који садржи само оне елементе x из a за које се може утврдити $\varphi(x, a)$. Пошто такав скуп мора бити јединствен, уводимо посебну ознаку за њега $\{x \mid x \in a \wedge \varphi(x, a)\}$ или $\{x \in a \mid \varphi(x, a)\}$. Приметимо да је $\{x \mid x \in a \wedge \varphi(x, a)\} \subseteq a$. Истичемо и следећу еквиваленцију:

$$t \in \{x \mid x \in a \wedge \varphi(x, a)\} \Leftrightarrow t \in a \wedge \varphi(t, a).$$

Теорема 13. *За сваки скуп a важи $\emptyset \subseteq a$.*

Доказ. Треба доказати формулу $\forall x(x \in \emptyset \Rightarrow x \in a)$. За било које x, формула $x \in \emptyset$ је еквивалентна са $\perp$, што значи да импликација $x \in \emptyset \Rightarrow x \in a$ мора бити еквивалентна са $\top$. Формални доказ формуле, правилима природне дедукције, остављен је за вежбу. □

Подсећамо на задатак 2, на страни 83, у коме је требало доказати: $\forall x \neg P(x) \vdash \forall x(P(x) \Rightarrow A(x))$

Пример 37. Полазећи од празног скупа $\emptyset$, наводимо неке од скупова које можемо изградити применом наведених аксиома.

Користећи аксиому пара добијамо скупове:

$\{\emptyset\}$, $\{\{\emptyset\}\}$, $\{\{\{\emptyset\}\}\}$, $\{\emptyset,\{\emptyset\}\}$, $\{\emptyset,\{\{\emptyset\}\}\}$, $\{\{\emptyset\},\{\{\emptyset\}\}\}$ итд.

Користећи аксиому партитивног скупа:

$\mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(\{\emptyset\}) = \{\emptyset,\{\emptyset\}\}$, $\mathcal{P}(\{\emptyset,\{\emptyset\}\}) = \{\emptyset,\{\emptyset\},\{\{\emptyset\}\},\{\emptyset,\{\emptyset\}\}\}$ итд.

Користећи аксиому издвајања, нпр. из скупа $\mathcal{P}(\{\emptyset,\{\emptyset\}\})$ формулом $\emptyset \in x \vee \{\emptyset\} \in x$ можемо „издвојити" скуп

$$\{x \mid x \in \mathcal{P}(\{\emptyset,\{\emptyset\}\}) \wedge (\emptyset \in x \vee \{\emptyset\} \in x)\} = \{\{\emptyset\},\{\{\emptyset\}\},\{\emptyset,\{\emptyset\}\}\}.$$

Применом аксиоме уније формирамо, нпр. скуп $\{\emptyset,\{\emptyset\},\{\{\emptyset\}\}\}$. Заиста, формирајмо синглтон $\{\emptyset\}$ и пар $\{\{\emptyset\},\{\{\emptyset\}\}\}$, а затим од ових скупова нови пар $\{\{\emptyset\},\{\{\emptyset\},\{\{\emptyset\}\}\}\}$. Тада је

$$\bigcup\{\{\emptyset\},\{\{\emptyset\},\{\{\emptyset\}\}\}\} = \{\emptyset,\{\emptyset\},\{\{\emptyset\}\}\}.$$

Слободније речено, ако су скупови задати навођењем елемената унутар витичастих заграда, онда $\bigcup a$ добијамо брисањем витичатих заграда које се односе на елементе скупа a (и избацивањем празног скупа уколико је он елемент од a): ако је $a = \{\{\emptyset\},\{\{\emptyset\},\{\{\emptyset\}\}\}\}$, онда је $\bigcup a = \{\emptyset,\{\emptyset\},\{\{\emptyset\}\}\}$.

До сада смо наведене аксиоме користили да бисмо доказали постојање извесних скупова. У наставку ћемо доказати нешто другачији резултат: да не постоји скуп који садржи све скупове.

Теорема 14. *Не постоји скуп који садржи све скупове.*

Доказ. Потребно је да из наведених аксиома изведемо формулу $\neg\exists y \forall x(x \in y)$. Уместо формалног извођења, наводимо само основне кораке доказа.

Претпоставимо супротно ономе што треба доказати, тј. да постоји скуп свих скупова, $\exists y \forall x(x \in y)$. Није тешко показати да овакав скуп v мора бити јединствен. Означимо са v такав скуп, $\forall x(x \in v)$. Према аксиоми издвајања, може се формирати скуп $u = \{x \mid x \in v \wedge x \notin x\}$. Из $\forall x(x \in u \Leftrightarrow x \in v \wedge x \notin x)$, изводимо

$$(*) \qquad u \in u \Leftrightarrow u \in v \wedge u \notin u.$$

Према закону искључења трећег, $u \in u$ или $u \notin u$.

Ако $u \in u$, користећи импликацију $u \in u \Rightarrow u \in v \wedge u \notin u$, добијену из $(*)$, изводимо $u \in v \wedge u \notin u$, тј. $u \notin u$. Контрадикција.

Нека $u \notin u$. Из $\forall x(x \in v)$ закључујемо да $u \in v$ (v садржи све скупове, па самим тим садржи и u), па имамо $u \in v \wedge u \notin u$.

Користећи импликацију $u \in v \wedge u \notin u \Rightarrow u \in u$, добијену из $(*)$, изводимо $u \in u$. Контрадикција.

Изведене контрадикције обарају полазну претпоставку да постоји скуп свих скупова. Дакле, $\neg \exists y \forall x (x \in y)$. □

Последица 1. *За сваки скуп постоји скуп који му не припада.*

Доказ. Тврђење следи из претходне теореме и Де Морганових закона за квантификаторе: $\neg \exists y \forall x (x \in y) \Leftrightarrow \forall y \exists x (x \notin y)$. □

За било који скуп a, унија $\bigcup a$ садржи само оне елементе који припадају бар једном елементу из a. Ако је a непразан скуп, онда из једног елемента скупа a можемо издвојити само оне елементе који припадају <u>свим</u> елементима из a:

$(\star)$ $$x \in \bigcap a \Leftrightarrow \forall t (t \in a \Rightarrow x \in t).$$

Овако одређен скуп $\bigcap a$ је јединствен и називамо га **пресеком** скупа a. Уместо $\bigcap a$ пише се и $\bigcap\limits_{t \in a} t$. Важно је имати на уму да је дефинисан само пресек <u>непразног</u> скупа. Пресек празног скупа није дефинисан, јер би се у том случају еквиваленцијом $(\star)$ тврдило да је $\bigcap \emptyset$ скуп свих скупова; једноставно је доказати формулу $\forall t (t \in \emptyset \Rightarrow x \in t)$).

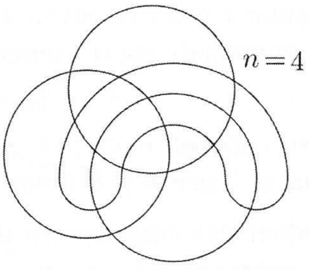
▼ Задаци и додаци

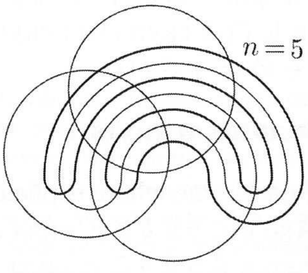
1. Која од следећих тврђења су тачна, за све a, b, c?
(а) Ако $a \in b$ и $b \in c$, онда $a \in c$.
(б) Ако $a \in b$ и $b \subseteq c$, онда $a \in c$.
(в) Ако $a \subseteq b$ и $b \in c$, онда $a \in c$.
(г) Ако $a \subseteq b$ и $b \subseteq c$, онда $a \subseteq c$.
2. Одредити следеће скупове:
(а) $\bigcup\{\{\emptyset\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\emptyset\}\}\}$
(б) $\bigcap\{\{\emptyset, \{\emptyset\}\}, \{\{\emptyset\}, \{\{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}\}$
3. Ако је $a \subseteq b$, доказати да је $\cup a \subseteq \cup b$, за све скупове a и b.
4. Доказати да за свако x, $x \subseteq \mathcal{P}(\cup x)$.
5. (а) Да ли за све скупове a и b важи еквиваленција: $\mathcal{P}(a) = \mathcal{P}(b)$ акко $a = b$? Образложити одговор.
(б) Да ли за све скупове a и b, из $\mathcal{P}(a) \in \mathcal{P}(b)$ следи $a \in b$?
6. Да ли за све скупове a и b важи еквиваленција: $\cup a = \cup b$ акко $a = b$? Образложити одговор.
7. Доказати за сваки непразан скуп X:
(а) ако је $x \subseteq a$, за свако $a \in X$, онда је $x \subseteq \bigcap X$;
(б) ако је $a \subseteq x$, за свако $a \in X$, онда је $\bigcup X \subseteq x$.
8. Скуп који садржи елементе свих својих елемената назива се *транзитиван* скуп, тј. T је транзитиван ако $\forall x (x \in T \Rightarrow x \subseteq T)$. Доказати, за сваки A:
(а) A је транзитиван акко је $\bigcup A \subseteq A$;
(б) Ако је A транзитиван, онда је $\bigcup A$ транзитиван;
(в) A је транзитиван акко је $A \subseteq \mathcal{P}(A)$.

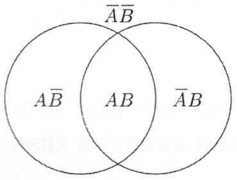
3.2. Основни концепти савремене математике

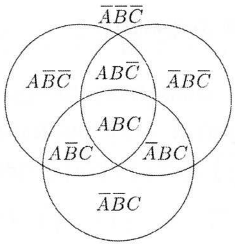
Увод. Покушаји да се визуелно представе поједине форме закључивања довели су до специфичних дијаграма који се везују за имена Ојлера, Вена, Пирса. Дијаграми које је проучавао Вен у свом раду из 1880. године, *О дијаграмској и механичкој репрезентацији исказа и закључивања*, данас су постали најпознатији графички прикази скупова. Укратко, Венов дијаграм је сачињен од коначно много затворених кривих линија приказаних у равни тако да сваку добијену област одређује јединствена комбинација унутрашњости и спољашњости тих кривих. Добро су познати прикази два, односно три скупа. Криву и њену унутрашњост означавамо истим словом, а спољашњост надвученим словом. Са повећањем броја скупова, прикази постају све сложенији: Венов дијаграм од n кривих дели раван на 2^n области. Често се у сложенијим случајевима изостављају надвучена слова (али се подразумевају).

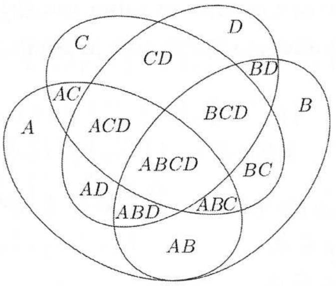
Леонард Ојлер (1707–1783), славни швајцарски математичар и физичар
Џон Вен (1834–1923), британски математичар и логичар
Чарлс Пирс (1839–1914), амерички логичар и филозоф











Вен је у поменутом раду приказао и један индуктиван начин генерисања дијаграма, приказан на маргини.

План

- Булове операције: унија, пресек, разлика, комплемент
- уређен пар, уређена тројка, уређена четворка, итд.
- Декартов производ; Декартов степен
- релација између два скупа: празна релација, пуна релација, дијагонала скупа
- функција између два скупа: празна функција, идентичка функција
- композиција релација, композиција функција
- инверзна релација; проблем инверзне функције: 1-1 функција, на функција, бијекција
- особине бинарне релације скупа: рефлексивност, ирефлексивност, симетричност, антисиметричност, транзитивност, линеарност
- релација еквиваленције: класа еквиваленције, количнички скуп
- релација уређења: строго уређење, (парцијално) уређење, линарно (тотално) уређење
- највећи и најмањи елемент уређења; максималан и минималан елемент уређења

▼ Булове (скуповне) операције

Лема 6. *Следећа тврђења су последице уведених аксиома:*

1. $\forall A \forall B \exists! Y \forall x (x \in Y \Leftrightarrow x \in A \wedge x \in B)$

2. $\forall A \forall B \exists! Y \forall x (x \in Y \Leftrightarrow x \in A \wedge x \notin B)$

3. $\forall A \forall B \exists! Y \forall x (x \in Y \Leftrightarrow x \in A \vee x \in B)$

Доказ. Тврђења 1) и 2) су директне последице схеме издвајања и аксиоме екстензионалности узимајући да је $\varphi_1(x, A, B)$ формула $x \in B$, одн. да је $\varphi_2(x, A, B)$ формула $x \notin B$:

$$\forall A \forall B \exists! Y \forall x (x \in Y \Leftrightarrow \underbrace{x \in A \wedge x \in B}_{x \in A \wedge \varphi_1(x,A,B)}), \text{ одн. } \forall A \forall B \exists! Y \forall x (x \in Y \Leftrightarrow \underbrace{x \in A \wedge x \notin B}_{x \in A \wedge \varphi_2(x,A,B)})$$

3) Нека је $Y = \bigcup\{A, B\}$. За било које x имамо[96]:

$$\begin{aligned} x \in Y &\Leftrightarrow x \in \bigcup\{A, B\} \\ &\Leftrightarrow \exists t (t \in \{A, B\} \wedge x \in t) \\ &\Leftrightarrow \exists t ((t = A \vee t = B) \wedge x \in t) \\ &\Leftrightarrow \exists t ((t = A \wedge x \in t) \vee (t = B \wedge x \in t)) \\ &\Leftrightarrow \exists t (t = A \wedge x \in t) \vee \exists t (t = B \wedge x \in t) \\ &\Leftrightarrow x \in A \vee x \in B. \end{aligned}$$

Дакле, за дате скупове A и B, постојање и јединственост скупа Y следи из аксиома екстензионалности, пара и уније. □

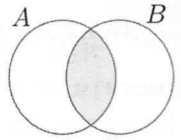
[96] У еквиваленцијском ланцу користимо формулу:

$$\exists t (t = A \wedge x \in t) \Leftrightarrow x \in A,$$

коју није тешко доказати, користећи правило:

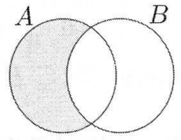
$$\frac{\varphi[x/u] \quad u = v}{\varphi[x/v]}$$

Дефиниција 8. *1)* ***Пресек*** *скупова A и B јесте скуп $A \cap B$ који садржи само оне елементе који припадају и скупу A и скупу B, и других елемената осим ових нема. Пресек скупова A и B означавамо $A \cap B$: $A \cap B = \{x \mid x \in A \wedge x \in B\}$. Скупови A и B су* ***дисјунктни*** *ако је $A \cap B = \emptyset$.*

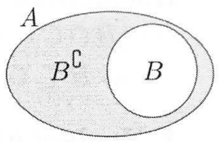


$A \cap B$

2) ***Разлика*** *скупова A и B јесте скуп који садржи само оне елементе који припадају скупу A, а не припадају скупу B, и других елемената осим ових нема. Специјално, ако је $B \subseteq A$, разлику $A \setminus B$ називамо* ***комплементом*** *скупа B у односу на A. Када је у неком контексту јасно у односу на који скуп A се одређују комплементи, онда уместо $A \setminus B$ пишемо $B^{\complement}$.*

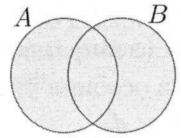


$A \setminus B$



3) ***Унија*** *скупова A и B јесте скуп $A \cup B$ који садржи само оне елементе који припадају скупу A или скупу B (бар једном од скупова A, B), и других елемената осим ових нема:*

$$A \cup B = \bigcup\{A, B\} = \{x \mid x \in A \vee x \in B\}.$$



$A \cup B$

Теорема 15. *За произвољне скупове A, B, C важи:*

1. $A \cap A = A$	2. $A \cup A = A$
3. $A \cap B = B \cap A$	4. $A \cup B = B \cup A$
5. $A \cap (B \cap C) = (A \cap B) \cap C$	6. $A \cup (B \cup C) = (A \cup B) \cup C$
7. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	8. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
9. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$	10. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

Доказ. Све наведене једнакости једноставно доказујемо формирањем еквиваленцијских ланаца у којима користимо одговарајуће теореме предикатског рачуна. Наводимо само неколико доказа, а остале остављамо за вежбу.

Једнакост (1) $A \cap A = A$ потврђује следећи ланац (у коме користимо $\vdash \alpha \wedge \alpha \Leftrightarrow \alpha$):

$$x \in A \cap A \Leftrightarrow x \in A \wedge x \in A \Leftrightarrow x \in A.$$

Једнакост (8) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ потврђује ланац:

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow x \in A \vee x \in B \cap C \Leftrightarrow x \in A \vee (x \in B \wedge x \in C) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in A \vee x \in C) \\ &\qquad\qquad [\vdash \alpha \vee (\beta \wedge \gamma) \Leftrightarrow (\alpha \vee \beta) \wedge (\alpha \vee \beta)] \\ &\Leftrightarrow x \in A \cup B \wedge x \in A \cup C \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

Једнакост (10) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ потврђује ланац:

$$\begin{aligned} x \in A \setminus (B \cup C) &\Leftrightarrow x \in A \wedge \neg x \in B \cup C \Leftrightarrow x \in A \wedge \neg(x \in B \vee x \in C) \\ &\Leftrightarrow x \in A \wedge (\neg x \in B \wedge \neg x \in C) \\ &\qquad\qquad [\vdash \neg(\alpha \vee \beta) \Leftrightarrow \neg\alpha \wedge \neg\beta] \\ &\Leftrightarrow (x \in A \wedge \neg x \in B) \wedge (x \in A \wedge \neg x \in C) \\ &\qquad\qquad [\vdash \alpha \wedge (\beta \wedge \gamma) \Leftrightarrow (\alpha \wedge \beta) \wedge (\alpha \wedge \gamma)] \\ &\Leftrightarrow x \in A \setminus B \wedge x \in A \setminus C \\ &\Leftrightarrow x \in (A \setminus B) \cap (A \setminus C). \end{aligned}$$

Корисно је приметити да сваком од наведених скуповних идентитета одговара једна сродна таутологија. □

Последица 2. *Ако је $B \subseteq A$ и $C \subseteq A$, онда је:*
(1) $(B \cap C)^{\complement} = B^{\complement} \cup C^{\complement}$ и $(B \cup C)^{\complement} = B^{\complement} \cap C^{\complement}$,
(2) из $B \subseteq C$ следи $C^{\complement} \subseteq B^{\complement}$.

▼ Уређен пар. Декартов производ два скупа

Уређен пар скупова a и b, у ознаци (a, b) представља целину коју чине a и b, наведени одређеним редоследом – зна се који објекат је *први* (леви) члан целине, а који је *други* (десни) члан целине. Кључна особина уређених парова јесте да из $(a, b) = (c, d)$ следи $a = c$ и $b = d$.

Дефиниција 9. *Уређен пар скупова a и b, у ознаци (a, b) јесте скуп $\{\{a\}, \{a, b\}\}$, при чему је a прва координата и b друга координата.*

$(a, b) \overset{\text{def}}{=} \{\{a\}, \{a, b\}\}$

Теорема 16. *Нека су a, b, c и d било који скупови. Тада:*

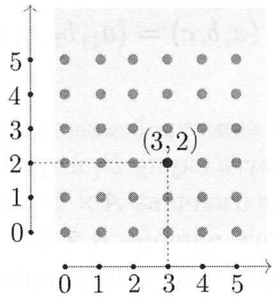
$$(a, b) = (c, d) \Leftrightarrow a = c \wedge b = d.$$

$\{a, b\} = \{c, d\} \Leftrightarrow (a = c \wedge b = d)$
$\vee\ (a = b \wedge b =$

Доказ. Посебно доказујемо сваку импликацију.
($\Leftarrow$) Ако је $a = c$ и $b = d$, онда је $\{a\} = \{c\}$ и $\{a, b\} = \{c, d\}$, па је и $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$, тј. $(a, b) = (c, d)$.
($\Rightarrow$) Нека је $(a, b) = (c, d)$, тј. $\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$. Знамо да су два скупа једнака ако имају исте елементе, па из претпостављене једнакости закључујемо да важе једнакости наведене у сваком од следећа два случаја. Доказаћемо да у оба случаја мора бити $a = c$ и $b = d$.
1. случај: $\{a\} = \{c\}$, $\{a, b\} = \{c, d\}$. Из $\{a\} = \{c\}$ следи да је $a = c$, а одатле и из $\{a, b\} = \{c, d\}$, да је и $b = d$.
2. случај: $\{a\} = \{c, d\}$, $\{a, b\} = \{c\}$. Из $\{a\} = \{c, d\}$ следи да је $a = c = d$, а из $\{a, b\} = \{c\}$ да је $a = b = c$. Самим тим, свакако важи $a = c$ и $b = d$. □

Лема 7. *За свака два скупа A и B постоји јединствени скуп који садржи уређене парове чије прве координате припадају скупу A, а друге координате припадају скупу B (и других елемената нема):*

$$\forall A \forall B \exists ! Y \forall x (x \in Y \Leftrightarrow \exists a \exists b (a \in A \wedge b \in B \wedge x = (a, b)))$$



Доказ. Скуп $\mathcal{P}(\mathcal{P}(A \cup B))$ садржи све уређене парове чије прве координате припадају скупу A, а друге координате припадају скупу B. Заиста,

ако $a \in A$ и $b \in B$,	тада	$a, b \in A \cup B$,
	одакле следи	$\{a\}, \{a, b\} \subseteq A \cup B$,
	тј.	$\{a\}, \{a, b\} \in \mathcal{P}(A \cup B)$.
	па даље имамо	$\{\{a\}, \{a, b\}\} \subseteq \mathcal{P}(A \cup B)$,
	односно	$(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$.

Наравно, скуп $\mathcal{P}(\mathcal{P}(A \cup B))$ садржи и свакакве друге елементе (који нису уређени парови, као и уређене парове чије координате не испуњавају постављени услов), па је потребно применити аксиому издвајања да бисмо формирали тражени (јединствен) скуп:

$$Y = \{x \mid x \in \mathcal{P}(\mathcal{P}(A \cup B)) \wedge \exists a \exists b (a \in A \wedge b \in B \wedge x = (a, b))\}.$$

Посебно истичемо да су у доказу овог тврђења употребљене аксиоме екстензионалности, пара, уније, партитивног скупа и схема издвајања. □

Дефиниција 10. ***Декартов производ*** *скупова A и B јесте скуп уређених парова чије прве координате припадају скупу A, а друге скупу B. Декартов производ скупова A и B означавамо $A \times B$ и пишемо:*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Рене Декарт (1596–1650), славни француски математичар и филозоф

Пример 38. Декартов производ скупова $A = \{0, 1, 2\}$ и $B = \{0, 1\}$ јесте скуп $A \times B = \{(0,0), (0,1), (1,0), (1,1), (2,0), (2,1)\}$. Приметимо да је $B \times A = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$, као и да је $A \times B \neq B \times A$.

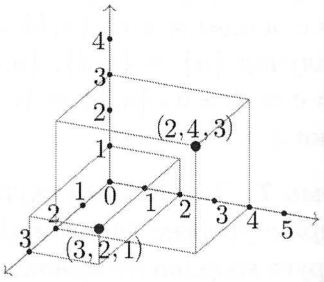
Бројеве $0, 1, 2$ можемо схватити као ознаке међусобно различитих скупова; нпр. $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$.

Можемо формирати и следеће Декартове производе:
$A \times A = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2),(2,0),(2,1),(2,2)\}$,
$B \times B = \{(0,0),(0,1),(1,0),(1,1)\}$.

Будући да празан скуп нема елементе, не можемо формирати уређене парове чија једна координата долази из празног скупа. Одавде следи да за сваки скуп A важе једнакости

$$A \times \emptyset = \emptyset = \emptyset \times A.$$

▼ Уређене тројке, четворке, ... Декартови производи и степени



За произвољне a, b, c, **уређену тројку** (a,b,c) дефинишемо на следећи начин: $(a,b,c) \stackrel{\text{def}}{=} ((a,b),c)$, при чему a, b, c редом називамо првом, другом, трећом координатом уређене тројке (a,b,c). Следећи еквиваленцијски ланац доказује основну особину уређених тројки:

$$\begin{aligned}(a,b,c) = (a_1,b_1,c_1) \;&\Leftrightarrow\; (a,b) = (a_1,b_1) \land c = c_1\\ &\Leftrightarrow\; a = a_1 \land b = b_1 \land c = c_1.\end{aligned}$$

Скуп свих уређених тројки чија прва координата припада скупу A, друга скупу B, и трећа скупу C јесте скуп $(A \times B) \times C$, који се краће означава $A \times B \times C$. Слично као за Декартове производе два скупа, пишемо $A \times B \times C = \{(a,b,c) \mid a \in A \land b \in B \land c \in C\}$.

$(A \times B) \times C$ и $A \times (B \times C)$ нису једнаки скупови, па зато у запису $A \times B \times C$ не изостављамо заграде због асоцијативности, већ по договору. Према општем договору о изостављању заграда, приликом означавања Декартовог производа подразумева се да је $A_1 \times A_2 \times A_3 \times \cdots \times A_n$ краћи запис за

$(\cdots((A_1 \times A_2) \times A_3) \times \cdots) \times A_n$,

а не да се заграде могу постављати произвољно.

Потпуно аналогно уводимо уређене четворке, петорке итд:

$$(a,b,c,d) \stackrel{\text{def}}{=} ((a,b,c),d),\ (a,b,c,d,e) \stackrel{\text{def}}{=} ((a,b,c,d),e),\ \ldots,$$

и Декартове производе више од три скупа:

$$A \times B \times C \times D = \{(a,b,c,d) \mid a \in A \land b \in B \land c \in C \land d \in D\}, \ldots$$

Ако је A било који скуп, Декартове производе

$$A \times A,\ A \times A \times A,\ A \times A \times A \times A,\ \text{итд.}$$

називамо **Декартовим степенима** и краће их означавамо A^2, A^3, A^4 итд.

▼ Релације између два скупа: празна релација, пуна релација, дијагонала скупа

Да бисмо поједноставили записивање формула, усвајамо следеће договоре: за било коју формулу α,
- $(\forall x \in X)\,\alpha$ означава $\forall x(x \in X \Rightarrow \alpha)$;
- $(\exists x \in X)\,\alpha$ означава $\exists x(x \in X \land \alpha)$;
- $(\exists! x \in X)\,\alpha$ означава $\exists! x(x \in X \land \alpha)$.

Приметимо да се за било коју формулу α једноставно доказује $(\forall x \in \emptyset)\alpha$.

Није тешко доказати следећу еквиваленцију

$$(\exists! x \in X)\,\alpha \Leftrightarrow (\exists x \in X)\,\alpha \land (\forall x_1 \in X)(\forall x_2 \in X)(\alpha[x/x_1] \land \alpha[x/x_2] \Rightarrow x_1 = x_2).$$

Следеће скраћенице примењујемо у обичном тексту:

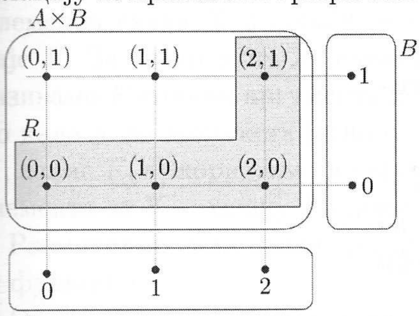
„за сваки $x \in X$"	значи	„за сваки x који припада X";
„постоји $x \in X$"	значи	„постоји x који припада X";
„скуп $X \subseteq A$"	значи	„скуп X који је подскуп скупа A".

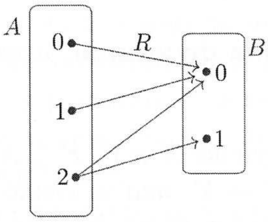
Дефиниција 11. *Сваки подскуп од $X \times Y$ назива се* **бинарна релација** *између X и Y. Специјално, подскуп од $X \times X$ назива се бинарна релација скупа X.*

Дакле, $\mathcal{P}(X \times Y)$ је скуп свих релација између X и Y. Посебно,

- $\emptyset$ је тзв. *празна* релација између било која два скупа X и Y ($\emptyset \subseteq X \times Y$);
- $X \times Y$ је тзв. *пуна* релација између X и Y ($X \times Y \subseteq X \times Y$).

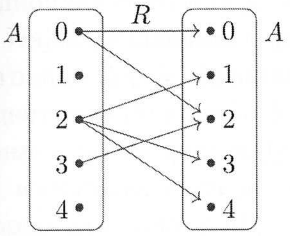
Пример 39. Ако је $A = \{0,1,2\}$ и $B = \{0,1\}$, онда је скуп $R = \{(0,0),(1,0),(2,0),(2,1)\}$ једна бинарна релација између A и B. У једноставним случајевима, као што је овај, погодно је релацију R приказати графички:

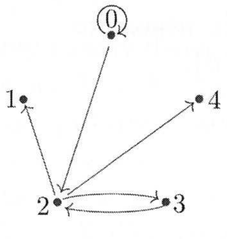




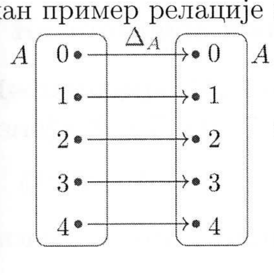
Наводимо још неколико релација између A и B: $P = \{(1,2)\}$, $Q = \{(0,0),(0,1)\}$, $S = \{(0,1),(1,1),(2,1)\}$ итд.

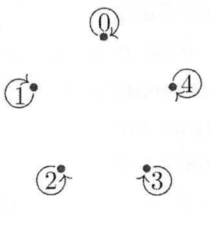
Пример 40. Нека је R нека релација скупа A, $R \subseteq A \times A$. Да бисмо графички приказали R не морамо два пута цртати скуп A. На пример, релацију $R = \{(0,0),(0,2),(2,1),(2,3),(2,4),(3,2)\}$ скупа $A = \{0,1,2,3,4\}$ графички можемо приказати као на наредним сликама.





Релација $\Delta_A = \{(0,0),(1,1),(2,2),(3,3),(4,4)\} \subseteq A \times A$ је важан пример релације скупа A – назива се *дијагонала скупа* A.





Дефиниција 12. ***Дијагонала*** *скупа X је скуп*

$$\Delta_X = \{(x,y) \mid (x,y) \in X \times X \land x = y\} = \{(x,x) \mid x \in X\}.$$

Није тешко аксиомама оправдати постојање скупа Δ_X. Из скупа $X \times X$ издвајамо (ослањајући се, наравно, на схему издвајања) уређене парове чије су координате исте.

$$\{z \in X \times X \mid (\exists x \in X)\, z = (x,x)\}$$

Сваки скуп R чији су елементи уређени парови јесте заправо бинарна релација скупа $\bigcup\bigcup R$. Заиста, координате било ког пара (a,b) из R припадају $\bigcup\bigcup R$: ако $(a,b) = \{\{a\},\{a,b\}\} \in R$, онда $\{a\},\{a,b\} \in \bigcup R$, па $a,b \in \bigcup\bigcup R$. Дакле, сваки скуп R који садржи само уређене парове можемо сматрати бинарном релацијом: $R \subseteq (\bigcup\bigcup R) \times (\bigcup\bigcup R)$. Скуп свих првих координата уређених парова из R назива се **домен** релације R и обележава се $\mathrm{dom}(R)$, а скуп свих других координата назива се **кодомен** релације R и обележава $\mathrm{codom}(R)$ или $\mathrm{ran}(R)$.

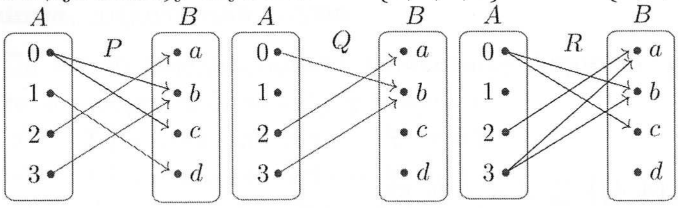
$$\mathrm{dom}(R) = \{a \in \bigcup\bigcup R \mid \exists b\,(b \in \bigcup\bigcup R \land (a,b) \in R)\}$$
$$\mathrm{ran}(R) = \{b \in \bigcup\bigcup R \mid \exists a\,(a \in \bigcup\bigcup R \land (a,b) \in R)\}$$

▼ Функција између два скупа (празна функција, идентичка функција)

Дефиниција 13. *Релација F између скупова X и Y, $F \subseteq X \times Y$ је* ***функција*** *из X у Y, у ознаци $F : X \to Y$, ако за свако x из X постоји јединствено y из Y тако да $(x,y) \in F$, тј. важе следећи услови:*
(F1) *за свако $x \in X$ постоји $y \in Y$ тако да $(x,y) \in F$,*
(F2) *за свако $x \in X$ и све $y_1, y_2 \in Y$, из $(x,y_1) \in F$ и $(x,y_2) \in F$ следи $y_1 = y_2$.*

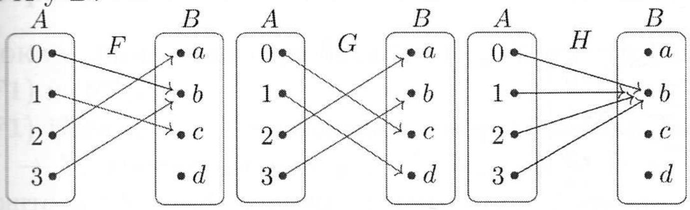
Према претходној дефиницији, запис $F : X \to Y$ је скраћење за формулу $(\forall x \in X)(\exists! y \in Y)(x,y) \in F$, односно за конјункцију следеће две формуле:
(F1) $(\forall x \in X)(\exists y \in Y)(x,y) \in F$,
(F2) $(\forall x \in X)(\forall y_1 \in Y)(\forall y_2 \in Y)((x,y_1) \in F \land (x,y_2) \in F \Rightarrow y_1 = y_2)$.

Пример 41. На наредним сликама представљено је неколико релација између скупова $A = \{0,1,2,3\}$ и $B = \{a,b,c,d\}$.



Релације P, Q и R нису функције из A у B. Релација P не испуњава услов **(F2)**, према коме елемент домена не може бити почетак више од једне стрелице: $(0,b) \in P$, $(0,c) \in P$ и $b \neq c$. Релација Q не испуњава услов **(F1)**, према коме сваки елемент домена мора бити почетак неке стрелице: елемент 1 није прва координата ниједног уређеног пара из Q. Релација R не задовољава ни услов **(F1)** ни **(F2)**.

Релације F, G и H, приказане на сликама испод јесу функције из A у B.



Ове функције краће описујемо следећим табелама:

$$F = \begin{pmatrix} 0 & 1 & 2 & 3 \\ b & c & a & b \end{pmatrix}, G = \begin{pmatrix} 0 & 1 & 2 & 3 \\ c & d & a & b \end{pmatrix}, H = \begin{pmatrix} 0 & 1 & 2 & 3 \\ b & b & b & b \end{pmatrix}.$$

Ако $F : X \to Y$, уместо $(x, y) \in F$ пишемо $F(x) = y$ или $x \overset{F}{\mapsto} y$. Елементи скупа X називају се *оригинали* или *аргументи* функције F. За сваки x из X, елемент y из Y такав да је $F(x) = y$ називамо *F-сликом* аргумента x, при чему префикс F изостављамо када је из контекста јасно о којој функцији F је реч. За x из X, запис $F(x)$ користимо и самостално као ознаку одговарајућег елемента из Y – ознаку F-слике елемента x.

Размотримо када *празна релација* и *пуна релација* представљају функције.

(1) Да ли је $\emptyset$, посматран као празна релација између скупова X и Y, функција из X у Y? Одговор је:
– Не, уколико је $X \neq \emptyset$, јер није задовољен услов (**F1**);
– Да, уколико је $X = \emptyset$. Није тешко показати да услови (**F1**) и (**F2**) важе када се уместо X и F стави $\emptyset$:
(**F1**) $(\forall x \in \emptyset)(\exists y \in Y)(x, y) \in \emptyset$,
(**F2**) $(\forall x \in \emptyset)(\forall y_1 \in Y)(\forall y_2 \in Y)((x, y_1) \in \emptyset \wedge (x, y_2) \in \emptyset \Rightarrow y_1 = y_2)$.

(2) Да ли је пуна релација $X \times Y$, између скупова X и Y, функција из X у Y? Одговор је потврдан само у случају да је Y једночлан скуп или је $X = \emptyset$.[109]

Најзад издвајамо и једну важну функцију било ког скупа. Дијагонала Δ_X је функција из X у X, $\Delta_X : X \to X$ и назива се *идентичка функција*. У литератури се користи доста различитих ознака за ову функцију: id_X, I_X, Id_X, 1_X итд, при чему се индекс X изоставља када је јасно на који скуп X се односи. Ми ћемо користити ознаку $\mathrm{id}_X : X \to X$. Приметимо да је $\mathrm{id}_X(x) = x$, за свако $x \in X$.

[109] Приметимо да за сваки скуп X, постоји само једна функција из X у неки једночлан скуп.

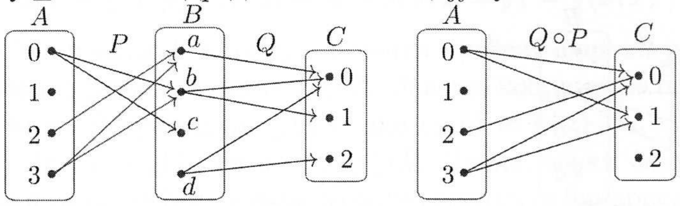
▼ Композиција релација. Композиција функција

Дефиниција 14. *Нека је $R \subseteq X \times Y$ и $Q \subseteq Y \times Z$. Релација између X и Z, $Q \circ R \subseteq X \times Z$ дата са*

$$Q \circ R = \{(x, z) \in X \times Z \mid (\exists y \in Y)\,((x, y) \in R \wedge (y, z) \in Q)\}$$

назива се ***композиција*** *релација R и Q.*

Пример 42. На слици доле лево дате су две релације $P \subseteq A \times B$ и $Q \subseteq B \times C$. Одредимо композицију $Q \circ P$.



Ослањајући се на дате графове релација уочавамо да (x, z) припада релацији $Q \circ P$ ако постоји стрелица из x у неки елемент скупа B и стрелица из тог истог елемента у z, тј. ако су x и z повезани двема надовезаним стрелицама (крај једне стрелице поклапа се са почетком друге стрелице).

Теорема 17. *Нека је* $R \subseteq X \times Y$, $Q \subseteq Y \times Z$ *и* $P \subseteq Z \times U$. *Тада је:*
(1) $R \circ \Delta_X = R = \Delta_Y \circ R$,
(2) $P \circ (Q \circ R) = (P \circ Q) \circ R$.

Доказ. (1) Очигледно су $R \circ \Delta_X$ и $\Delta_Y \circ R$ подскупови од $X \times Y$. Доказе жељених једнакости наводимо у облику следећих еквиваленцијских ланаца:

Подсећамо на правило:

$$\frac{\varphi[x/u] \quad u = v}{\varphi[x/v]}$$

$$\begin{aligned}(x,y) \in R \circ \Delta_X &\Leftrightarrow (\exists t \in X)((x,t) \in \Delta_X \wedge (t,y) \in R)\\ &\Leftrightarrow (\exists t \in X)(x = t \wedge (t,y) \in R)\\ &\Leftrightarrow (x,y) \in R\end{aligned}$$

$$\begin{aligned}(x,y) \in \Delta_Y \circ R &\Leftrightarrow (\exists t \in Y)((x,t) \in R \wedge (t,y) \in \Delta_Y)\\ &\Leftrightarrow (\exists t \in Y)((x,t) \in R \wedge t = y)\\ &\Leftrightarrow (x,y) \in R\end{aligned}$$

(2)[112] Нека је $R \subseteq X \times Y$, $Q \subseteq Y \times Z$ и $P \subseteq Z \times U$. Тада је $Q \circ R \subseteq X \times Z$, па је $P \circ (Q \circ R) \subseteq X \times U$. Такође, $P \circ Q \subseteq Y \times U$, па је $(P \circ Q) \circ R \subseteq X \times U$. Остаје још да за сваки уређени пар (x, u) из $X \times U$ докажемо еквиваленцију:
$(x,u) \in P \circ (Q \circ R) \Leftrightarrow (x,u) \in (P \circ Q) \circ R$:

$$\begin{aligned}(x,u) \in P \circ (Q \circ R) &\Leftrightarrow (\exists z \in Z)(\underline{(x,z) \in Q \circ R} \wedge (z,u) \in P)\\ &\Leftrightarrow (\exists z \in Z)(\underline{(\exists y \in Y)((x,y) \in R \wedge (y,z) \in Q)} \wedge (z,u) \in P)\\ &\Leftrightarrow (\exists z \in Z)(\exists y \in Y)((x,y) \in R \wedge (y,z) \in Q \wedge (z,u) \in P)\\ &\Leftrightarrow (\exists y \in Y)\underline{(\exists z \in Z)}((x,y) \in R \wedge \underline{(y,z) \in Q} \wedge \underline{(z,u) \in P})\\ &\Leftrightarrow (\exists y \in Y)((x,y) \in R \wedge \underline{\exists z(z \in Z \wedge (y,z) \in Q \wedge (z,u) \in P)})\\ &\Leftrightarrow (\exists y \in Y)((x,y) \in R \wedge \underline{(y,u) \in P \circ Q})\\ &\Leftrightarrow (x,u) \in (P \circ Q) \circ R\end{aligned}$$

Доказана особина оправдава запис $P \circ Q \circ R$, без заграда. □

[112] У доказу користимо:
(1) $\vdash \exists v(\alpha \wedge \beta) \Leftrightarrow \alpha \wedge \exists v \beta$, када се променљива v не појављује слободно у формули α,
(2) $\vdash \exists v_1 \exists v_2 \varphi \Leftrightarrow \exists v_2 \exists v_1 \varphi$, као и
(3) асоцијативност и комутативност конјункције.

Композиција две функције такође је функција.

Теорема 18. *Нека је $F : X \to Y$ и $G : Y \to Z$. Тада $G \circ F : X \to Z$.*

Доказ. Јасно је да мора бити $G \circ F \subseteq X \times Z$. Проверимо услове (**F1**) и (**F2**).

(**F1**) Нека је $x \in X$ произвољно изабран елемент. Будући да $F : X \to Y$, постоји елемент $y \in Y$ такав да је $(x, y) \in F$. Даље, пошто $G : Y \to Z$, постоји елемент $z \in Z$ такав да је $(y, z) \in G$. Одавде, следи да $(x, z) \in G \circ F$.

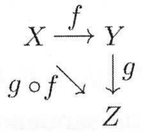
(**F2**) Нека су $x \in X$, $z_1, z_2 \in Z$ произвољно изабрани елементи, такви да је $(x, z_1) \in G \circ F$ и $(x, z_2) \in G \circ F$.

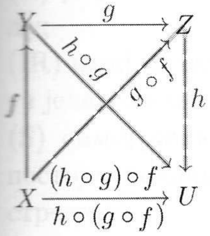
Из $(x, z_1) \in G \circ F$ следи да постоји $y_1 \in Y$ такав да $(x, y_1) \in F$ и $(y_1, z_1) \in G$.

Из $(x, z_2) \in G \circ F$ следи да постоји $y_2 \in Y$ такав да $(x, y_2) \in F$ и $(y_2, z_2) \in G$.

Пошто $F : X \to Y$, из $(x, y_1) \in F$ и $(x, y_2) \in F$, закључујемо да $y_1 = y_2$. Најзад, пошто $G : Y \to Z$, из $y_1 = y_2$, $(y_1, z_1) \in G$ и $(y_2, z_2) \in G$, закључујемо да $z_1 = z_2$. □

Ако $f : X \to Y$ и $g : Y \to Z$, тада за x из X, елемент $(g \circ f)(x)$, тј. $g \circ f$-слику елемента x означавамо $g(f(x))$.





Према теореми 17 (2), ако $f : X \to Y$, $g : Y \to Z$ и $h : Z \to U$, једнакост

$$(h \circ g) \circ f = h \circ (g \circ f)$$

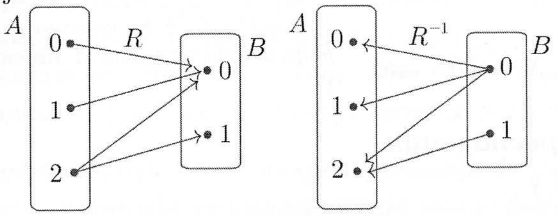
допушта да композицију ове три функције означавамо $h \circ g \circ f : X \to U$.

▼ Инверзна релација. 1-1 функција, на-функција, бијекција

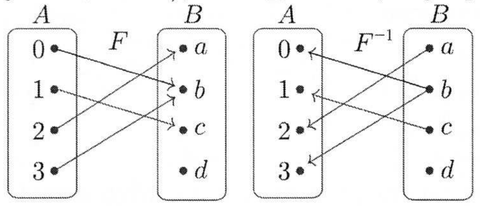
Дефиниција 15. *Нека је $R \subseteq X \times Y$. Релација $R^{-1} \subseteq Y \times X$ дата са $R^{-1} = \{(y, x) \mid (x, y) \in R\}$ назива се* ***инверзна релација*** *релације R.*

Пример 43. Нека је $A = \{0, 1, 2\}$ и $B = \{0, 1\}$.

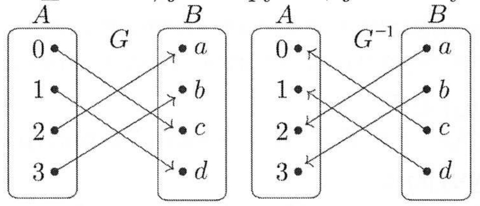
Ако је $R \subseteq A \times B$ и $R = \{(0, 0), (1, 0), (2, 0), (2, 1)\}$, онда је $R^{-1} \subseteq B \times A$ и $R^{-1} = \{(0, 0), (0, 1), (0, 2), (1, 2)\}$. Графички приказ релације R^{-1} добијамо променом смера свих стрелица релације R.



Пример 44. Инверзна релација функције <u>не мора</u> бити функција. Инверзна релација функције $F : A \to B$ (приказане на наредној слици лево), $F^{-1} \subseteq B \times A$, није функција из B у A.



Инверзна релација функције $G : A \to B$ (слика доле лево), $G^{-1} \subseteq B \times A$, јесте функција из B у A.



Ако $F : X \to Y$, релација $F^{-1} \subseteq Y \times X$ је функција из Y у X ако важи:

$(\forall y \in Y)(\exists! x \in X)(y, x) \in F^{-1}$, тј. $(\forall y \in Y)(\exists! x \in X)(x, y) \in F$.

Последња формула заправо обједињује следећа два услова:
(**F1**) $(\forall y \in Y)(\exists x \in X)(y, x) \in F^{-1}$,
(**F2**) $(\forall y \in Y)(\forall x_1 \in X)(\forall x_2 \in X)((y, x_1) \in F^{-1} \land (y, x_2) \in F^{-1} \Rightarrow x_1 = x_2)$.
Ако ова два услова преформулишемо на погодан начин, добијамо услове које мора да задовољава функција F да би њој инверзна релација такође била функција:
(**S**) $(\forall y \in Y)(\exists x \in X)(x, y) \in F$, тј. за свако y из Y постоји x из X такав да $(x, y) \in F$ (сваки y из Y јесте слика неког елемента из X);
(**I**) $(\forall y \in Y)(\forall x_1 \in X)(\forall x_2 \in X)((x_1, y) \in F \land (x_2, y) \in F \Rightarrow x_1 = x_2)$,
тј. ако x_1 и x_2 из X имају исте слике, онда су они једнаки.
Услов (**I**) можемо формулисати и у следећем облику:
(**I**) $(\forall x_1 \in X)(\forall x_2 \in X)(F(x_1) = F(x_2) \Rightarrow x_1 = x_2)$,
односно, ослањајући се на закон контрапозиције,
(**I**) $(\forall x_1 \in X)(\forall x_2 \in X)(x_1 \neq x_2 \Rightarrow F(x_1) \neq F(x_2))$.
Углавном ћемо користити једну од ове две последње формулације.

Дефиниција 16. *Нека* $F : X \to Y$.
- *F је **на-функција** или **сирјекција**, у ознаци* $F : X \overset{\text{na}}{\to} Y$, *ако задовољава услов* (**S**).[114]
- *F је **1-1 функција** или **инјекција**, у ознаци* $F : X \overset{1-1}{\to} Y$, *ако задовољава услов* (**I**).
- *F је **бијекција** или **обострано-једнозначна коресподенција**, у ознаци* $F : X \underset{\text{na}}{\overset{1-1}{\to}} Y$, *ако* $F : X \overset{1-1}{\to} Y$ *и* $F : X \overset{\text{na}}{\to} Y$.

На основу претходних разматрања изводимо следећи закључак.

[114] Ако $F : X \overset{\text{na}}{\to} Y$, кажемо да је F функција из скупа X **на** скуп Y.

Теорема 19. *Нека $F : X \to Y$.*
(1) *Инверзна релација функције F је функција акко је F бијекција.*
(2) *Ако је F бијекција, онда је и F^{-1} бијекција.*

Ако $F : X \to Y$, за y из Y смемо користити запис $F^{-1}(y)$ само ако знамо да је F бијекција, јер само тада то има смисла.

▾ Особине бинарних релација скупа

Дефиниција 17. *Нека је $R \subseteq X \times X$. Релација R је:*
(R) ***рефлексивна*** *ако је $\Delta_X \subseteq R$, тј. за свако $x \in X$, $(x, x) \in R$;*
(IR) ***ирефлексивна*** *ако је $\Delta_X \cap R = \emptyset$, тј. за свако $x \in X$ важи $(x, x) \notin R$;*
(S) ***симетрична*** *ако је $R \subseteq R^{-1}$, тј. за све $x, y \in X$, из $(x, y) \in R$ следи $(y, x) \in R$;*
(AS) ***антисиметрична*** *ако је $R \cap R^{-1} \subseteq \Delta_X$, тј. за све $x, y \in X$, из $(x, y) \in R$ и $(y, x) \in R$ следи $x = y$;*
(T) ***транзитивна*** *ако је $R \circ R \subseteq R$, тј. за све $x, y, z \in X$, из $(x, y) \in R$ и $(y, z) \in R$ следи $(x, z) \in R$;*
(L) ***линеарна*** *ако је $R \cup R^{-1} = X \times X$, тј. за све $x, y \in X$, $(x, y) \in R$ или $(y, x) \in R$.*

На графичким приказима бинарних релација неког скупа:
(R) рефексивност значи да уз сваки елемент треба нацртати петљу;
(IR) ирефексивност значи да петља не треба да буде нацртана ни уз један елемент;
(S) симетричност значи да између свака два елемента или не постоји ниједна стрелица или постоје две супротно оријентисане стрелице;
(AS) антисиметричност значи да између два различита елемента може постојати највише једна стрелица; присуство или одсуство петљи није повезано са особином антисиметричности;
(T) транзитивност значи да за сваке две надовезане стрелице (крај једне стрелице исти је као почетак друге стрелице), постоји стрелица која директно повезује почетак прве и крај друге;
(L) линеарност значи да између свака два елемента постоји бар једна стрелица и све петље.

▾ Релације еквиваленције: класе еквиваленције, количнички скуп

Једнакост је основна релација сваког непразног скупа. У универзуму скупова, бинарни предикат $=$ одређује на сваком непразном скупу X релацију једнакости, коју смо означавали Δ_X; природнија је ознака $=_X$, при чему је уобичајено да се изоставља индекс, јер је увек јасно који скуп се посматра.

Дефиниција 18. *Бинарна релација E скупа X, $E \subseteq X \times X$, јесте* ***релација еквиваленције*** *ако је рефлексивна, симетрична и транзитивна.*

Инфиксна нотација је много чешћа за бинарне релације; поред тога, релације еквиваленције се углавном означавају знацима који подсећају на знак једнакости, попут: $\approx, \sim, \cong, \simeq, \equiv, \doteq$, итд.

$$\frac{}{x \sim x} \qquad \frac{x \sim y}{y \sim x} \qquad \frac{x \sim y \quad y \sim z}{x \sim z}$$

Дефиниција 19. *Нека је $E \subseteq X \times X$ релација еквиваленције. За сваки елемент $x \in X$ скуп*

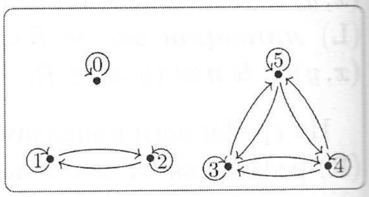
$$[x]_E = \{y \in X \mid (x, y) \in E\}$$

назива се ***класа еквиваленције*** *елемента x у односу на релацију E. Скуп свих класа еквиваленције назива се* ***количнички скуп*** *и обележава се X/E. Дакле,*

$$X/E = \{[x]_E \mid x \in X\}.$$

Класе еквиваленције се у литератури и другачије означавају. На пример, уместо $[x]_E$ пише се и x/E, или C_x у случајевима када је јасно о којој релацији еквиваленције је реч.

Пример 45. Релација E скупа $\{0,1,2,3,4,5\}$ задата је графом десно.



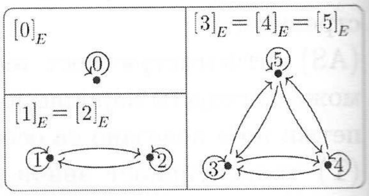
Није тешко уочити да је E релација еквиваленције. Одредимо класе еквиваленције релације:

$$[0]_E = \{0\}, [1]_E = [2]_E = \{1,2\}, [3]_E = [4]_E = [5]_E = \{3,4,5\}.$$

Количнички скуп је

$$\{0,1,2,3,4,5\}/E = \{[0]_E, [1]_E, [2]_E, [3]_E, [4]_E, [5]_E\} = \{\{0\}, \{1,2\}, \{3,4,5\}\}.$$

Очигледно да је класама еквиваленције скуп $\{0,1,2,3,4,5\}$ разбијен на непразне дисјунктне подскупове чија је унија наведени скуп.



Теорема 20. *Нека је $E \subseteq X \times X$ релација еквиваленције.*

1. *За свако $x \in X$, $x \in [x]_E$, па је самим тим $[x]_E \neq \emptyset$.*
2. *За све $x, y \in X$, $(x, y) \in E$ акко $[x]_E = [y]_E$.*
3. *За све $x, y \in X$, $[x]_E \neq [y]_E$ акко $[x]_E \cap [y]_E = \emptyset$.*
4. *$X = \bigcup X/E = \bigcup_{x \in X} [x]_E$.*

Доказ. 1. Тврђење следи директно из дефиниције класе еквиваленције и чињенице да је релација еквиваленције рефлексивна.

2. ($\Rightarrow$) Претпоставимо да $(x, y) \in E$. Треба доказати једнакост $[x]_E = [y]_E$.

Ако $z \in [x]_E$, онда $(x, z) \in E$. Због симетричности релације E, из $(x, y) \in E$ следи да $(y, x) \in E$. Како је E транзитивна релација из $(y, x) \in E$ и $(x, z) \in E$ следи $(y, z) \in E$, тј. $z \in [y]_E$. Дакле, $[x]_E \subseteq [y]_E$. Обрнута инклузија се доказује на исти начин.

($\Leftarrow$) Претпоставимо да је $[x]_E = [y]_E$. Због рефлексивности релације E имамо да $y \in [y]_E$, па $y \in [x]_E$ што значи да $(x, y) \in E$.

3. (⇒) Нека је $[x]_E \neq [y]_E$, тј. $(x, y) \notin E$ (према тврђењу под 2). Треба доказати да је $[x]_E \cap [y]_E = \emptyset$. Претпоставимо супротно, да је $[x]_E \cap [y]_E \neq \emptyset$, тј. да постоји z такав да је $z \in [x]_E \cap [y]_E$. Тада $z \in [x]_E$ и $z \in [y]_E$, тј. $(x, z) \in E$ и $(y, z) \in E$. Због симетричности релације E имамо да $(z, y) \in E$. Узимајући у обзир транзитивност релације E из $(x, z) \in E$ и $(z, y) \in E$ закључујемо да $(x, y) \in E$ што је супротно полазној претпоставци.

(⇐) Претпоставимо да је $[x]_E \cap [y]_E = \emptyset$. Уколико би било $[x]_E = [y]_E$, имали бисмо да је $[x]_E = [y]_E = [x]_E \cap [y]_E = \emptyset$, што је немогуће према тврђењу под 1. Дакле, $[x]_E \neq [y]_E$. □

▼ Уређења: строга, парцијална, линеарна

Дефиниција 20. *Релација $R \subseteq X \times X$ је:*
- ***релација строгог поретка**, односно **строго уређење** ако је ирефлексивна и транзитивна;*
- ***релација поретка**, односно **(парцијално) уређење** ако је рефлексивна, антисиметрична и транзитивна;*
- ***релација линеарног поретка**, односно **линеарно (тотално) уређење** ако је рефлексивна, антисиметрична, транзитивна и линеарна.*

Теорема 21. [120] *1) Ако је $\preccurlyeq$ уређење скупа X, онда је релација $\prec$ дата са:*

$$x \prec y \text{ акко } x \preccurlyeq y \wedge x \neq y,$$

строго уређење скупа X.
2) Ако је $\prec$ строго уређење скупа X, онда је релација $\preccurlyeq$ дата са:

$$x \preccurlyeq y \text{ акко } x \prec y \vee x = y,$$

уређење скупа X.

[120] Ако је нека релација поретка приказана графички, брисањем свих петљи добијамо одговарајућу релацију строгог поретка. Важи и обрнуто, додавањем свих петљи на приказ релације строгог поретка, добијамо приказ одговарајуће релације поретка.

Доказ. 1) (IR) Релација $\prec$ је ирефлексивна, јер је конјункција $x \preccurlyeq x \wedge x \neq x$ нетачна за свако x.

(T) Нека је $x \prec y$ и $y \prec z$. Тада је

$$x \preccurlyeq y, x \neq y, y \preccurlyeq z, y \neq z.$$

Како је $\preccurlyeq$ транзитивна, из $x \preccurlyeq y$ и $y \preccurlyeq z$, следи да је $x \preccurlyeq z$. Остаје још да се докаже да је $x \neq z$. Претпоставимо супротно, да је $x = z$. Тада је $x \preccurlyeq y$ и $y \preccurlyeq x$, па због антисиметричности релације $\preccurlyeq$ важи $x = y$, што није могуће јер је $x \neq y$.

2) (R) Релација $\preccurlyeq$ је рефлексивна, јер за свако x важи $x = x$, а самим тим и $x \prec x \vee x = x$.

(AS) Претпоставимо да је $x \preccurlyeq y$ и $y \preccurlyeq x$. Треба да докажемо да је $x = y$. Претпоставимо супротно да је $x \neq y$. Тада мора бити $x \prec y$ и $y \prec x$. Међутим, из транзитивности релације $\prec$ следи да је $x \prec x$, што није могуће, јер је $\prec$ ирефлексивна релација.

(T) Претпоставимо да је $x \preccurlyeq y$ и $y \preccurlyeq z$. Треба доказати да је $x \preccurlyeq z$. Разликујемо неколико случајева.

1. случај. Ако је $x = y$ и $y = z$, онда је $x = z$, па важи $x \preccurlyeq z$.
2. случај. Ако је $x \prec y$ и $y = z$, онда је и $x \prec z$, па је $x \preccurlyeq z$.
3. случај. Ако је $x = y$ и $y \prec z$, онда је и $x \prec z$, па је $x \preccurlyeq z$.
4. случај. Ако је $x \prec y$ и $y \prec z$, онда због транзитивности релације $\prec$ важи $x \prec z$, а самим тим и $x \preccurlyeq z$. □

Релације строгог поретка углавном се означавају знацима попут $<$, $\prec$, $\lhd$, $\sqsubset$ и слично, а њима одговарајуће релације поретка додавањем цртице испод знака: $\leqslant$ (или $\leq$), $\preceq$ (или $\preccurlyeq$), $\unlhd$, $\sqsubseteq$. У наставку ћемо овај договор о означавању подразумевати.

Пример 46. За било који скуп X, инклузија одређује једну релацију поретка на скупу $\mathcal{P}(X)$:
(R) за све $A \in \mathcal{P}(X)$ важи $A \subseteq A$,
(AS) за све $A, B \in \mathcal{P}(X)$, из $A \subseteq B$ и $B \subseteq A$ следи $A = B$,
(T) за све $A, B, C \in \mathcal{P}(X)$, из $A \subseteq B$ и $B \subseteq C$ следи $A \subseteq C$.

Строга инклузија ($\subset$) је строго уређење на $\mathcal{P}(X)$.

Дефиниција 21. *Нека је $\leqslant$ релација поретка на скупу X.*
- *Елемент $a \in X$ је $\leqslant$-**најмањи** ако <u>за свако</u> $x \in X$ важи $a \leqslant x$.*
- *Елемент $a \in X$ је $\leqslant$-**највећи** ако <u>за свако</u> $x \in X$ важи $x \leqslant a$.*
- *Елемент $a \in X$ је $\leqslant$-**минималан** ако <u>не постоји</u> $x \in X$ такав да је $x < a$. (Наравно, $<$ означава строги поредак који одговара поретку $\leqslant$).*
- *Елемент $a \in X$ је $\leqslant$-**максималан** ако <u>не постоји</u> $x \in X$ такав да је $a < x$.*

У случајевима када је јасно за коју релацију поретка $\leqslant$ одређујемо елементе уведене претходном дефиницијом, у називима тих елемената изостављамо префикс „$\leqslant$-".

▼ Важни примери функција

Функције заузимају веома значајно место у свим математичким областима што донекле потврђује велики број синонима који се користе: пресликавања, трансформације, оператори итд.

Рестрикције. Ако $f : X \to Y$, тада је за сваки непразан подскуп A од X ($\emptyset \neq A \subseteq X$), скуп $f \cap (A \times Y)$ функција из A у Y. Ова функција се обележава $f\,|_A$ и назива **рестрикција** функције f на A. Дакле, $f\,|_A \colon A \to Y$. За $x \in A$, $f\,|_A (x) = f(x)$, док за $x \in X \setminus A$, запис $f\,|_A (x)$ нема смисла.

Пример 47. Нека $f : \{0,1,2,3\} \to \{a,b,c\}$:

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 \\ b & c & a & b \end{pmatrix}.$$

Тада је $f\,|_{\{0,1,2\}} = \begin{pmatrix} 0 & 1 & 2 \\ b & c & a \end{pmatrix}$, $f\,|_{\{1,3\}} = \begin{pmatrix} 1 & 3 \\ c & b \end{pmatrix}$, итд.

Лема 8. *Ако $f : X \to Y$ и $\emptyset \neq B \subseteq A \subseteq X$, онда је*

$$(f\,|_A)\,|_B = f\,|_B\,.$$

Доказ. Из $f|_A = f \cap (A \times Y)$ и $(f|_A)|_B = f|_A \cap (B \times Y)$ следи да је

$$(f|_A)|_B = f|_A \cap (B \times Y) = f \cap (A \times Y) \cap (B \times Y).$$

Како је $B \subseteq A$, онда је и $B \times Y \subseteq A \times Y$, тј. $(A \times Y) \cap (B \times Y) = B \times Y$. Дакле, $(f|_A)|_B = f \cap (B \times Y) = f|_B$. □

Пројекције. За било које скупове A и B, функције
- $\pi_A : A \times B \to A$, $\pi_A(x, y) = x$ и
- $\pi_B : A \times B \to B$, $\pi_B(x, y) = y$,

називају се *пројекције*.

Фактор пресликавање. Ако је E релација еквиваленције скупа X, функција $k : X \to X/E$, дефинисана са $k(x) = [x]_E$ назива се *количничко (фактор) пресликавање*.

Бинарне операције. Ако је S неки скуп, свака функција из $S \times S$ у S назива се *бинарна операција* скупа S.

Пример 48. Бинарну операцију $* : \{0, 1, 2\} \times \{0, 1, 2\} \to \{0, 1, 2\}$ скупа $\{0, 1, 2\}$ дату са

$$* = \begin{pmatrix} (0,0) & (0,1) & (0,2) & (1,0) & (1,1) & (1,2) & (2,0) & (2,1) & (2,2) \\ 0 & 0 & 1 & 1 & 2 & 0 & 0 & 2 & 1 \end{pmatrix}$$

представљамо и тзв. Кејлијевом таблицом.

Артур Кејли (1821–1895), енглески математичар

$*$	0	1	2
0	0	0	1
1	1	2	0
2	0	2	1

Уместо $*(x, y)$ пише се $x * y$.

Уобичајено је да се бинарне операције означавају разним специјалним симболима $+$, $\cdot$, $*$, $\star$, $\oplus$ итд, као и да се користи тзв. *инфиксна нотација* – ознаку операције наводимо између аргумената (за разлику од префиксне нотације где се ознака операције наводи испред аргумената).

Карактеристичне функције. Ако је S било који скуп, функције из S у двочлани скуп $\{0, 1\}$ представљају својеврсне репрезентације подскупова од S. Наиме, било који подскуп $A \subseteq S$ репрезентује његова *карактеристична функција* $\chi_A : S \to \{0, 1\}$,

$$\chi_A(x) = \begin{cases} 1, & x \in A, \\ 0, & x \notin A. \end{cases}$$

Ако 1 схватимо као „да" и 0 као „не" онда вредност $\chi_A(x)$ представља одговор на питање да ли x припада A.

Пример 49. Ако је $S = \{0, 1, 2, 3, 4\}$, онда је:

$$\chi_{\{0,2,4\}} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}, \; \chi_\emptyset = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ итд.}$$

Свака функција $f : S \to \{0,1\}$ одређује један подскуп скупа S чија је карактеристична функција управо f; реч је о подскупу $\{x \in S \mid f(x) = 1\}$.

Како за сваки $A \subseteq S$ важи $(\forall x \in S)(x \in A \Leftrightarrow \chi_A(x) = 1)$, закључујемо да су подскупови $A_1, A_2 \subseteq S$ једнаки ако и само ако $(\forall x \in S)(\chi_{A_1}(x) = \chi_{A_2}(x))$. Ово запажање може бити веома корисно приликом доказивања скуповних идентитета.

Посебно, свака бинарна релација скупа S, $R \subseteq S \times S$ може се посматрати и као функција $\chi_R : S \times S \to \{0,1\}$.

▼ Директне и индиректне слике

Било која функција $f : X \to Y$, одређује две нове функције:

- једну из $\mathcal{P}(X)$ у $\mathcal{P}(Y)$, коју називамо **ко-f** ('ко еф'), и за коју користимо исту ознаку f, али аргумент (подскуп од X) наводимо у угластим заградама:

$$f[A] \stackrel{\text{def}}{=} \{y \in Y \mid (\exists a \in A) f(a) = y\}, \text{ за } A \subseteq X.$$

- другу из $\mathcal{P}(Y)$ у $\mathcal{P}(X)$, коју називамо **контра-f** ('контра еф'), и за коју користимо ознаку f^{-1} (која у овом контексту нема никакве везе са појмом инверзне функције), а аргумент (подскуп од Y) наводимо у угластим заградама:

$$f^{-1}[B] \stackrel{\text{def}}{=} \{x \in X \mid f(x) \in B\}, \text{ за } B \subseteq Y.$$

Скуп $f[A] = \{y \in Y \mid (\exists a \in A) f(a) = y\} \subseteq Y$ називамо **директна слика** скупа $A \subseteq X$; $f[A]$ је подскуп од Y који садржи само оне елементе који су f-слике елемената из A. Будући да су сви елементи скупа $f[A]$ облика $f(a)$, $a \in A$, пишемо и $f[A] = \{f(a) \mid a \in A\}$.

Скуп $f^{-1}[B] = \{x \in X \mid f(x) \in B\} \subseteq X$ називамо **индиректна слика** скупа $B \subseteq Y$; $f^{-1}[B]$ је подскуп од X који садржи само оне елементе из X чије f-слике припадају скупу B.

Пример 50. Нека $f : \{0,1,2\} \to \{a,b,c\}$:

$$f = \begin{pmatrix} 0 & 1 & 2 \\ b & a & a \end{pmatrix}.$$

Одредимо директне слике свих подскупова домена:

$f[\emptyset] = \emptyset$ $\quad f[\{0\}] = \{b\}$ $\quad f[\{1\}] = \{a\}$ $\quad f[\{2\}] = \{a\}$

$f[\{0,1\}] = \{a,b\}$ $\quad f[\{1,2\}] = \{a\}$ $\quad f[\{0,2\}] = \{a,b\}$ $\quad f[\{0,1,2\}] = \{a,b\}$

Одредимо и индиректне слике свих подскупова кодомена:

$f^{-1}[\emptyset] = \emptyset$ $\quad f^{-1}[\{a\}] = \{1,2\}$ $\quad f^{-1}[\{b\}] = \{0\}$ $\quad f^{-1}[\{c\}] = \emptyset$

$f^{-1}[\{a,b\}] = \{0,1,2\}$ $\quad f^{-1}[\{a,c\}] = \{1,2\}$ $\quad f^{-1}[\{b,c\}] = \{0\}$ $\quad f^{-1}[\{a,b,c\}] = \{0,1,2\}$

Посебно наглашавамо да се, на пример, $f^{-1}[\{a\}]$ битно разликује од записа $f^{-1}(a)$, који у овом случају нема смисла јер f није бијекција.

Теорема 22. *Нека $f : X \to Y$. За произвољне $A, A_1, A_2 \subseteq X$ и $B, B_1, B_2 \subseteq Y$ важи:*

(1) $A \subseteq f^{-1}[f[A]]$; *(2)* $f[f^{-1}[B]] \subseteq B$;
(3) $A_1 \subseteq A_2 \Rightarrow f[A_1] \subseteq f[A_2]$; *(4)* $B_1 \subseteq B_2 \Rightarrow f^{-1}[B_1] \subseteq f^{-1}[B_2]$;
(5) $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$; *(6)* $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$;
(7) $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$; *(8)* $f^{-1}[B_1 \cup B_2] = f^{-1}[B_1] \cup f^{-1}[B_2]$.

ДОКАЗ. (1) Ако $x \in A$, онда је очигледно $f(x) \in f[A]$. Како је $f(x) \in f[A]$ еквивалентно са $x \in f^{-1}[f[A]]$, непосредно изводимо жељени закључак.
(2) Ако $y \in f[f^{-1}[B]]$, онда је $y = f(x)$, за неко $x \in f^{-1}[B]$. Како је $x \in f^{-1}[B]$ еквивалентно са $f(x) \in B$, следи $y = f(x) \in B$.
(3) Нека је $A_1 \subseteq A_2$. Претпоставимо да $y \in f[A_1]$. Тада је $y = f(x)$, за неко $x \in A_1$. Будући да је $A_1 \subseteq A_2$, из $y = f(x)$ и $x \in A_1 \subseteq A_2$ закључујемо да $y \in f[A_2]$.
(4) Нека је $B_1 \subseteq B_2$. Претпоставимо да $x \in f^{-1}[B_1]$, односно $f(x) \in B_1$. Из $f(x) \in B_1 \subseteq B_2$, закључујемо да $x \in f^{-1}[B_2]$.
(5) Ова инклузија директно следи из (3). Како је $A_1 \cap A_2 \subseteq A_1$ и $A_1 \cap A_2 \subseteq A_2$, из (3) следи $f[A_1 \cap A_2] \subseteq f[A_1]$ и $f[A_1 \cap A_2] \subseteq f[A_2]$, а одавде и $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$.
(6) Инклузију $f^{-1}[B_1 \cap B_2] \subseteq f^{-1}[B_1] \cap f^{-1}[B_2]$ директно добијамо из (4). Докажимо да је и $f^{-1}[B_1 \cap B_2] \supseteq f^{-1}[B_1] \cap f^{-1}[B_2]$. Ако $x \in f^{-1}[B_1] \cap f^{-1}[B_2]$, онда $x \in f^{-1}[B_1]$ и $x \in f^{-1}[B_2]$, односно $f(x) \in B_1$ и $f(x) \in B_2$. Дакле, $f(x) \in B_1 \cap B_2$, што је еквивалентно са $x \in f^{-1}[B_1 \cap B_2]$.
(7) Једнакост доказује следећи еквиваленцијски ланац:

$$\begin{aligned} y \in f[A_1 \cup A_2] &\Leftrightarrow \exists x(x \in A_1 \cup A_2 \wedge y = f(x)) \\ &\Leftrightarrow \exists x((x \in A_1 \vee x \in A_2) \wedge y = f(x)) \\ &\Leftrightarrow \exists x((x \in A_1 \wedge y = f(x)) \vee (x \in A_2 \wedge y = f(x)) \\ &\Leftrightarrow \exists x(x \in A_1 \wedge y = f(x)) \vee \exists x(x \in A_2 \wedge y = f(x)) \\ &\Leftrightarrow y \in f[A_1] \vee y \in f[A_2] \\ &\Leftrightarrow y \in f[A_1] \cup f[A_2]. \end{aligned}$$

(8) Једнакост доказује следећи еквиваленцијски ланац:

$$\begin{aligned} x \in f^{-1}[B_1 \cup B_2] &\Leftrightarrow f(x) \in B_1 \cup B_2 \\ &\Leftrightarrow f(x) \in B_1 \vee f(x) \in B_2 \\ &\Leftrightarrow x \in f^{-1}[B_1] \vee x \in f^{-1}[B_2] \\ &\Leftrightarrow x \in f^{-1}[B_1] \cup f^{-1}[B_2]. \quad \square \end{aligned}$$

▼ Задаци и додаци

1. Одредити следеће скупове навођењем његових елемената.
(а) $\{\emptyset\} \cap \{\emptyset, \{\emptyset\}\}$ (б) $\{\emptyset\} \cup \{\emptyset, \{\emptyset\}\}$
(в) $\{\emptyset\} \setminus \{\emptyset, \{\emptyset\}\}$ (г) $\mathcal{P}(\{\{\emptyset\}\})$
(д) $\mathcal{P}(\{\emptyset\} \cap \{\emptyset, \{\emptyset\}\})$ (ђ) $\mathcal{P}(\{\{\emptyset\}\}) \cap \{\emptyset, \{\emptyset\}\}$
(е) $\mathcal{P}(\{\emptyset, \{\emptyset\}\}) \cup \mathcal{P}(\{\emptyset\})$ (ж) $\mathcal{P}(\{\emptyset, \{\emptyset\}\}) \setminus \mathcal{P}(\{\emptyset\})$
(з) $\mathcal{P}(\emptyset) \times \mathcal{P}(\emptyset)$ (и) $\mathcal{P}(\{\emptyset\}) \times \mathcal{P}(\{\{\emptyset\}\})$

2. Које од следећих реченица су тачне за било које скупове A и B, а које не морају бити увек тачне?
i) Ако је $A \subseteq B$, онда је $A \cap B = B$.
ii) Ако је $A \cup \emptyset = \emptyset$, онда је $A = \emptyset$.
iii) Ако је $A \subseteq B$, онда је $B \setminus A = \emptyset$.
iv) Ако је $A \cap B = \emptyset$, онда је $A = \emptyset$ или $B = \emptyset$.
v) Ако је $A \cap B = A$, онда је $A \subseteq B$.
vi) Ако је $A \cup B = \emptyset$, онда је $A = \emptyset$ или $B = \emptyset$.
vii) Ако је $A \cup B = A \cap B$, онда је $A = B$.
viii) Ако је $A \setminus \emptyset = \emptyset$, онда је $A = \emptyset$.
ix) Ако је $A \cup B = A$, онда је $B \subseteq A$.
x) Ако је $A \setminus B \subseteq B$, онда је $A \subseteq B$.
xi) Ако је $A \cap B = \emptyset$, онда је $A \setminus B = A$.
xii) Ако је $A \cup B = \emptyset$, онда је $A \setminus B = \emptyset$.
xiii) Ако је $A \cap \emptyset = \emptyset$, онда је $A = \emptyset$.
xiv) Ако је $A \subseteq B$, онда је $A \setminus B = \emptyset$.
xv) Ако је $A \cap B = A$, онда је $A = B$.

3. Доказати да за произвољне скупове A, B, C важи:
(а) $A \cap B \subseteq A$, $A \cap B \subseteq B$
(б) $A \subseteq A \cup B$, $B \subseteq A \cup B$
(в) Ако је $C \subseteq A$ и $C \subseteq B$, онда је $C \subseteq A \cap B$
(г) Ако је $A \subseteq C$ и $B \subseteq C$, онда је $A \cup B \subseteq C$
(д) Ако је $B \subseteq C$, онда је $A \setminus C \subseteq A \setminus B$

4. Доказати да за све скупове X и Y важи:
(а) $\mathcal{P}(X \cap Y) = \mathcal{P}(X) \cap \mathcal{P}(Y)$; (б) $\mathcal{P}(X \cup Y) \subseteq \mathcal{P}(X) \cup \mathcal{P}(Y)$.

5. Навести пример скупова X и Y, ако је то могуће, таквих да је $\mathcal{P}(X \cup Y) \neq \mathcal{P}(X) \cup \mathcal{P}(Y)$.

6. Доказати да су следећи услови међусобно еквивалентни:
(1) $A \subseteq B$ (2) $A \cup B = B$ (3) $A \cap B = A$ (4) $A \setminus B = \emptyset$

7. Ако је $A \cup B = A \cap B$, доказати да је $A = B$.

8. (а) Доказати природном дедукцијом

$$r \Rightarrow p \vdash (p \wedge q) \vee r \Leftrightarrow p \wedge (q \vee r).$$

(б) Да ли за произвољне скупове P, Q, R важи еквиваленција:

$$(P \cap Q) \cup R = P \cap (Q \cup R) \Leftrightarrow R \subseteq P?$$

9. (а) Доказати $p \wedge \neg r \vdash (p \wedge \neg q) \vee (q \vee \neg r)$.
(б) Ако су P, Q, R произвољни скупови доказати да је

$$P \setminus R \subseteq (P \setminus Q) \cup (Q \setminus R).$$

(в) Доказати да је $P \setminus R \subseteq (P \setminus Q) \cup (Q \setminus R)$ акко $R \subseteq Q \subseteq P$.

10. Симетрична разлика скупова A и B јесте скуп

$$A \triangle B \stackrel{\text{def}}{=} (A \setminus B) \cup (B \setminus A).$$

Доказати да за све A, B, C важи:
(а) $A \triangle B = B \triangle A$
(б) $A \triangle (B \triangle C) = (A \triangle B) \triangle C$

(в) $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$
(г) $A \triangle (A \triangle B) = B$
(д) $A \cup B = (A \triangle B) \triangle (A \cap B)$
(ђ) $A \setminus B = A \triangle (A \cap B)$
(е) $A \triangle A = \emptyset$
(ж) $A \triangle \emptyset = A$

11. Доказати: $A \triangle B = C \Leftrightarrow B \triangle C = A \Leftrightarrow C \triangle A = B$.

12. (а) Доказати да скуп $[x,y] \stackrel{\text{def}}{=} \{\{x,y\},\{y\}\}$, има основно својство уређених парова:

(∗) $$[x_1,y_1] = [x_2,y_2] \Leftrightarrow x_1 = x_2 \wedge y_1 = y_2.$$

(б) Који од следећих скупова има својство (∗):
1. $[x,y] \stackrel{\text{def}}{=} \{\{\emptyset,x\},\{\{\emptyset\},y\}\}$;
2. $[x,y] \stackrel{\text{def}}{=} \{\{x\},\{y\}\}$;
3. $[x,y] \stackrel{\text{def}}{=} \{x,\{y\}\}$?

13. Доказати да за све скупове A, B, C важе једнакости:
(а) $A \times (B \cup C) = (A \times B) \cup (A \times C)$
(б) $A \times (B \cap C) = (A \times B) \cap (A \times C)$
(в) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

14. Доказати да за произвољне скупове A, B, C, D важи:
(а) $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$
(б) $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$

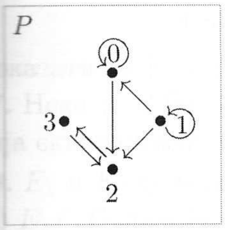
15. Које услове треба да задовољавају скупови A, B, C, D да би важило $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$?

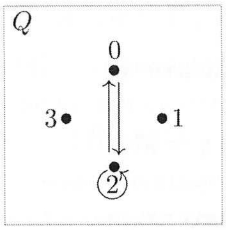
16. Навести пример скупова X, Y, Z, ако је то могуће, тако да је $X \cup (Y \times Z) \neq (X \cup Y) \times (X \cup Z)$.

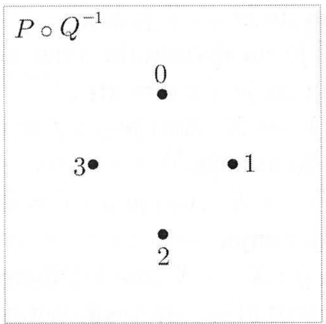
17. Нека је $R, R_1 \subseteq X \times Y$ и $Q, Q_1 \subseteq Y \times Z$.
(а) Ако је $R \subseteq R_1$, онда је $Q \circ R \subseteq Q \circ R_1$.
(б) Ако је $Q \subseteq Q_1$, онда је $Q \circ R \subseteq Q_1 \circ R$.

18. Нека су P, Q, R бинарне релације скупа S. Доказати:
(а) $P \circ (Q \cup R) = (P \circ Q) \cup (P \circ R)$ $\quad (Q \cup R) \circ P = (Q \circ P) \cup (Q \circ P)$
(б) $P \circ (Q \cap R) \subseteq (P \circ Q) \cap (P \circ R)$ $\quad (Q \cap R) \circ P \subseteq (Q \circ P) \cap (R \circ P)$
(в) $(P \cup Q)^{-1} = P^{-1} \cup Q^{-1}$ $\quad (P \cap Q)^{-1} = P^{-1} \cap Q^{-1}$

19. На сликама су приказане две бинарне релације P и Q, скупа $\{0,1,2,3\}$. Нацртати граф релације $P \circ Q^{-1}$.







20. Нека је B бинарна релација скупа S. Доказати да је $B = \Delta_S$ акко $B \circ R = R \circ B = R$, за сваку бинарну релацију R скупа S.

21. Који од скупова
$f_1 = \{(1,a),(2,b),(3,c),(4,c),(5,d),(6,d)\}$
$f_2 = \{(1,a),(2,b),(3,c),(3,d),(4,d),(5,c),(6,d)\}$
$f_3 = \{(1,b),(2,c),(3,a),(5,d)\}$
$f_4 = \{(1,b),(2,b),(3,b),(4,b),(5,b),(6,b)\}$
$f_5 = \{(1,d),(3,c),(4,c),(2,b),(5,c),(6,c)\}$
јесте функција из $A = \{1,2,3,4,5,6\}$ у $B = \{a,b,c,d\}$?
22. Одредити све функције скупа $A = \{0,1\}$ у скуп $\{a,b,c\}$.
23. Нека је X било који скуп који има бар два елемента и нека је $F : X \times X \to \mathcal{P}(X)$ функција дата са $F(x,y) = X \setminus \{x,y\}$, за $(x,y) \in X \times X$. Да ли је F 1-1 функција? Да ли је F на функција? Детаљно образложити одговоре.
24. Нека је $\emptyset \neq A \subset B$ (тј. A је непразан, строги подскуп скупа B) и $F : \mathcal{P}(B) \to \mathcal{P}(A)$ функција дата са $F(X) = X \cap A$, за $X \in \mathcal{P}(B)$. Да ли је F 1-1 функција? Да ли је F на функција? Детаљно образложити одговоре.
25. Нека је $A, B \subseteq S \neq \emptyset$. Функција $f : \mathcal{P}(S) \to \mathcal{P}(A) \times \mathcal{P}(B)$ дефинисана је на следећи начин: $f(X) = (X \cap A, X \cap B)$. Доказати да је f 1-1 функција акко је $S = A \cup B$.
26. За дате функције $f : A \to B$ и $g : C \to D$, дефинисана је функција $h : A \times C \to B \times D$,

$$h(x,y) \stackrel{\text{def}}{=} (f(x), g(y)),\ (x,y) \in A \times C.$$

(а) Ако су f и g 1-1 функције, да ли и h мора бити 1-1 функција?
(б) Ако су f и g на функције, да ли и h мора бити на функција?
27. Нека $f : X \to Y$ и $g : Y \to Z$.
(а) Ако $f : X \stackrel{1-1}{\to} Y$ и $g : Y \stackrel{1-1}{\to} Z$, онда $g \circ f : X \stackrel{1-1}{\to} Z$.
(б) Ако $f : X \stackrel{\text{na}}{\to} Y$ и $g : Y \stackrel{\text{na}}{\to} Z$, онда $g \circ f : X \stackrel{\text{na}}{\to} Z$.
(в) Ако $f : X \underset{\text{na}}{\stackrel{1-1}{\to}} Y$ и $g : Y \underset{\text{na}}{\stackrel{1-1}{\to}} Z$, онда $g \circ f : X \underset{\text{na}}{\stackrel{1-1}{\to}} Z$.
28. Нека је $f : X \to Y$. Доказати:
(а) $f : X \stackrel{1-1}{\to} Y$ акко за све $g, h : Z \to X$, из $f \circ g = f \circ h$ следи $g = h$;
(б) $f : X \stackrel{\text{na}}{\to} Y$ акко за све $g, h : Y \to Z$, из $g \circ f = h \circ f$ следи $g = h$.
29. Функција $f : X \to Y$ је 1-1 функција акко постоји бар једна функција $g : Y \to X$ таква да је $g \circ f = \mathrm{id}_X$.
30. Функција $f : X \to Y$ је на функција акко постоји бар једна функција $g : Y \to X$ таква да је $f \circ g = \mathrm{id}_Y$.
31. Нека $f : X \to Y$ и $g : Y \to X$. Ако је $g \circ f = \mathrm{id}_X$, доказати да је f 1-1 функција, а g на функција.
32. Нека $f : X \to Y$ и $g : Y \to X$. Ако је $g \circ f = \mathrm{id}_X$ и $f \circ g = \mathrm{id}_Y$, доказати да су и g и f бијекције.
33. Нека су $f : X \to X$ и $g : X \to X$ две 1-1 функције. Ако важи услов $(\forall x \in X)\,(f(x) = x \vee g(x) = x)$, доказати да је $f \circ g = g \circ f$.
34. Нека је $F \subseteq X \times Y$ и $F^{-1} \subseteq Y \times X$ одговарајућа инверзна релација. Доказати да $F : X \to Y$ ако и само ако $\Delta_X \subseteq F^{-1} \circ F$ и

$F \circ F^{-1} \subseteq \Delta_Y$.

35. Нека $F : X \to Y$. Доказати:

(а) $F : X \overset{1-1}{\to} Y$ акко $\Delta_X = F^{-1} \circ F$;

(б) $F : X \overset{\text{na}}{\to} Y$ акко $\Delta_Y = F \circ F^{-1}$;

(в) $F : X \underset{\text{na}}{\overset{1-1}{\to}} Y$ акко $\Delta_X = F^{-1} \circ F$ и $\Delta_Y = F \circ F^{-1}$.

36. Нека су A, B, C, D непразни скупови, $f : A \to B$, $g : B \to C$ и $h : C \to D$. Ако су $g \circ f$ и $h \circ g$ бијекције, доказати да су све три функције f, g, h такође бијекције.

37. Ако је могуће, навести пример бинарне релације неког скупа која је:

(а) рефлексивна и симетрична, али није транзитивна;

(б) рефлексивна и антисиметрична, али није транзитивна;

(в) рефлексивна и транзитивна, али није симетрична;

(г) антисиметрична и транзитивна, али није рефлексивна.

38. Ако је релација симетрична и антисиметрична, доказати да је транзитивна.

39. Нека је R релација скупа S. Доказати да је R рефлексивна и транзитивна акко је $R = (R \circ R) \cup \Delta_S$.

40. Ако су R_1 и R_2 рефлексивне (ирефлексивне) релације, испитати да ли су рефексивне (ирефлексивне) релације $R_1 \cup R_2$, $R_1 \cap R_2$, R_1^{-1}, $R_1 \circ R_2$.

41. Ако су R_1 и R_2 симетричне релације, испитати да ли су симетричне релације $R_1 \cup R_2$, $R_1 \cap R_2$, R_1^{-1}, $R_1 \circ R_2$.

42. Ако су R_1 и R_2 симетричне релације, доказати да је производ $R_1 \circ R_2$ симетрична релација акко је $R_1 \circ R_2 = R_2 \circ R_1$.

43. R_1 и R_2 су антисиметричне релације скупа S. Доказати да је:

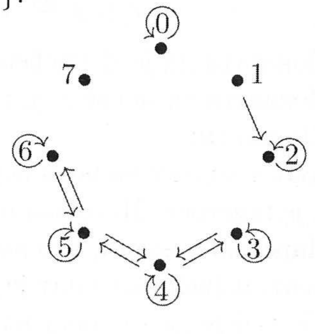
(а) R_1^{-1} антисиметрична релација;

(б) $R_1 \cap R_2$ антисиметрична релација;

(в) $R_1 \cup R_2$ антисиметрична релација акко је $R_1 \circ R_2^{-1} \subseteq \Delta_S$.

44. Доказати да је једнакост (Δ_S) једина бинарна релација скупа S која је истовремено и релација еквиваленције и уређење.

45. На слици десно је приказана релација на скупу $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Доцртати најмањи број стрелица, и навести одговарајуће уређене парове тако да добијени граф представља релацију еквиваленције датог скупа. Одредити затим класе еквиваленције.



46. Нека је $C \subseteq S$. На скупу $\mathcal{P}(S)$ дефинисана је релација:

$$A \sim B \overset{\text{def}}{=} A \triangle B \subseteq C, \; A, B \in \mathcal{P}(S).$$

Доказати да је $\sim$ релација еквиваленције на $\mathcal{P}(S)$.

47. Нека је R бинарна релација скупа S. Доказати да је R релација еквиваленције акко је $(R \circ R^{-1}) \cup \Delta_S = R$.

48. E_1 и E_2 су релације еквиваленције на скупу S. Доказати да је:

(а) $E_1 \cap E_2$ такође релација еквиваленције скупа S;

(б) $E_1 \cup E_2$ релација еквиваленције скупа S акко је $E_1 \cup E_2 = E_1 \circ E_2$;

(в) $E_1 \circ E_2$ релација еквиваленције скупа S акко је $E_1 \circ E_2 = E_2 \circ E_1$.

49. Нека су E_1 и E_2 две релације еквиваленције скупа S такве

да је $S/E_1 = S/E_2$. Доказати да је $E_1 = E_2$.

Додатак

Партиција (или **разбијање**) скупа S је скуп $\Pi \subseteq \mathcal{P}(S)$ који задовољава следеће услове:
(1) за свако $X \in \Pi$ важи $X \neq \emptyset$;
(2) за све $X, Y \in \Pi$, ако је $X \neq Y$, онда је $X \cap Y = \emptyset$;
(3) $S = \bigcup \Pi$.

Према теореми 20, свака релација еквиваленције E на неком скупу A одређује партицију A/E скупа A.

50. За сваку партицију Π скупа S, доказати да постоји јединствена релација еквиваленције E таква да је $\Pi = S/E$.

51. Ако је R уређење скупа S, доказати да је R^{-1} и уређење на S.

52. Нека су $<_A$ и $<_B$ строга уређења редом скупова A и B. Доказати да је релација $<_{\text{lex}}$ скупа $A \times B$, дефинисана са:

$$(a_1, b_1) <_{\text{lex}} (a_2, b_2) \stackrel{\text{def}}{=} a_1 <_A a_2 \vee (a_1 = a_2 \wedge b_1 <_B b_2),$$

строго уређење $A \times B$.

Напомена. Уређење $<_{\text{lex}}$ се назива *лексикографско уређење.*

53. Нека су $\leqslant_A$ и $\leqslant_B$ два линеарна уређења редом скупова A и B. Доказати да је релација $\leqslant$ скупа $A \times B$, дефинисана са:

$$(a_1, b_1) \leqslant (a_2, b_2) \stackrel{\text{def}}{=} a_1 \leqslant_A a_2 \wedge b_1 \leqslant_B b_2,$$

уређење $A \times B$. Примером показати да ово уређење не мора бити линеарно.

54. Нека је $* : X \times X \to X$ бинарна операција на скупу X, таква да за све $x, y, z \in X$ важи:
(I) $x * x = x$
(K) $x * y = y * x$
(A) $x * (y * z) = (x * y) * z$.

Бинарна релација $\leq$ скупа X дефинисана је на следећи начин:

$$x \leq y \stackrel{\text{def}}{\Leftrightarrow} x * y = x, \quad x, y \in X.$$

(а) Доказати да је $\leq$ уређење.
(б) Доказати да за све $x, y, z \in X$, из $z \leq x$ и $z \leq y$ следи $z \leq x * y$.

55. Доказати:
(а) Ако, у односу на неки поредак, постоји најмањи елемент, онда је он јединствен. Исто важи и за највећи елемент.
(б) Најмањи елемент, ако постоји, уједно је и (једини) минималан елемент; највећи елемент је једини максималан елемент.
(в) Могуће је да у односу на неко уређење постоји више минималних, одн. максималних елемената.

56. Одредити најмањи, минималан, највећи, максималан елемент, када такви елементи постоје, у скупу:
(а) $\mathcal{P}(\{0,1,2\})$ уређеном инклузијом $\subseteq$;
(б) $\mathcal{P}(\{0,1,2\}) \setminus \{\emptyset\}$ уређеном инклузијом $\subseteq$;

(в) $\mathcal{P}(\{0,1,2\}) \setminus \{\{0,1,2\}\}$ уређеном инклузијом $\subseteq$;
(г) $\mathcal{P}(\{0,1,2\}) \setminus \{\emptyset, \{0,1,2\}\}$ уређеном инклузијом $\subseteq$.

57. Нека $f : X \to Y$. Доказати:
(а) f је 1-1 функција акко за свако $A \subseteq X$, $A = f^{-1}[f[A]]$;
(б) f је на функција акко за свако $B \subseteq Y$, $f[f^{-1}[B]] = B$.

58. Нека је $f : X \to Y$. Доказати да за све $A \subseteq X$ и $B \subseteq Y$:
(а) $f[A] \cap B = f[A \cap f^{-1}[B]]$;
(б) $f[A] \subseteq B$ акко $A \subseteq f^{-1}[B]$.

59. (а) Ако $f : X \overset{1-1}{\to} Y$, да ли ко-функција $f[\cdot] : \mathcal{P}(X) \to \mathcal{P}(Y)$ мора такође бити 1-1 функција?
(б) Ако $f : X \overset{1-1}{\to} Y$, да ли контра-функција $f^{-1}[\cdot] : \mathcal{P}(Y) \to \mathcal{P}(X)$ мора такође бити 1-1 функција?

60. Фиксна тачка функције $g : X \to X$ јесте сваки елемент a из X такав да је $g(a) = a$. Нека је G скуп свих фиксних тачака функције g. Ако функција $f : X \to X$ комутира са g, тј. ако је $f \circ g = g \circ f$, доказати да је $f[G] \subseteq G$.

ДОДАТАК

Ако је $\mathcal{A}$ непразан скуп и $A : I \to \mathcal{A}$, директна слика $A[I]$ се некада назива и *фамилија* скупова из $\mathcal{A}$, индексирана елементима скупа I. Тада се уместо $A(i)$ пише A_i, и при тој нотацији је $A[I] = \{A_i \mid i \in I\}$. Природно је за сваку фамилију $\{A_i \mid i \in I\}$ посматрати *унију*, у ознаци $\bigcup_{i\in I} A_i$, и *пресек*, у ознаци $\bigcap_{i\in I} A_i$: $\bigcup_{i\in I} A_i = \bigcup A[I]$ и $\bigcap_{i\in I} A_i = \bigcap A[I]$.
Приметимо и следеће:

$$
\begin{aligned}
x \in \bigcup_{i\in I} A_i \Leftrightarrow x \in \bigcup A[I] \\
\Leftrightarrow \exists X\,(X \in A[I] \land x \in X) \\
\Leftrightarrow \exists X\,((\exists i \in I)\, X = A(i) \land x \in X) \\
\Leftrightarrow (\exists i \in I)\, \exists X\,(X = A_i \land x \in X) \\
\Leftrightarrow (\exists i \in I)\, x \in A_i
\end{aligned}
$$

$$
\begin{aligned}
x \in \bigcap_{i\in I} A_i \Leftrightarrow x \in \bigcap A[I] \\
\Leftrightarrow \forall X\,(X \in A[I] \Rightarrow x \in X) \\
\Leftrightarrow \forall X\,((\exists i \in I)\, X = A(i) \Rightarrow x \in X) \\
\Leftrightarrow \forall X\,(\forall i \in I)\,(X = A_i \Rightarrow x \in X) \\
\Leftrightarrow (\forall i \in I)\, \forall X\,(X = A_i \Rightarrow x \in X) \\
\Leftrightarrow (\forall i \in I)\, x \in A_i
\end{aligned}
$$

---

61. Нека $f : X \to Y$. Доказати:
(а) За било коју фамилију A_i, $i \in I$ подскупова од X важи:

$$f\left[\bigcup_{i\in I} A_i\right] = \bigcup_{i\in I} f[A_i] \quad \text{и} \quad f\left[\bigcap_{i\in I} A_i\right] \subseteq \bigcap_{i\in I} f[A_i].$$

(б) За било коју фамилију B_i, $i \in I$ подскупова од Y важи:

$$f^{-1}\left[\bigcup_{i\in I} B_i\right] = \bigcup_{i\in I} f^{-1}[B_i] \quad \text{и} \quad f^{-1}\left[\bigcap_{i\in I} B_i\right] = \bigcap_{i\in I} f^{-1}[B_i].$$

3.3. ZF теорија

Увод. **ZF** теорија представља списак аксиома којима се изражавају основна својства скупова. Име теорије потиче од почетних слова презимена двојице немачких математичара, Цермела и Френкела који су дали завршни облик теорије. Подсећамо, аксиоме описујемо на предикатском језику са два бинарна предиката: $\in$ (припадање) и $=$ (једнакост).

Ернст Цермело (1871–1953), немачки математичар
Абрахам Френкел (1891–1965), израелски математичар

Аксиома екстензионалности. Два скупа су једнака ако и само ако имају исте елементе.

$\forall a \forall b (a = b \Leftrightarrow \forall x (x \in a \Leftrightarrow x \in b))$

Аксиома празног скупа. Постоји скуп који нема елемената.

$\exists y \forall x (x \in y \Leftrightarrow \bot)$

Аксиома пара. За свака два скупа a_1 и a_2 постоји скуп y чији су једини елементи a_1 и a_2.

$\forall a_1 \forall a_2 \exists y \forall x (x \in y \Leftrightarrow x = a_1 \vee x = a_2)$

Аксиома уније. За сваки скуп a постоји скуп који садржи све елементе елемената скупа a и других елемената нема.

$\forall a \exists y \forall x (x \in y \Leftrightarrow \exists t (t \in a \wedge x \in t))$

Аксиома партитивног скупа. За сваки скуп a постоји скуп који садржи све подскупове скупа a и других елемената нема.

$\forall a \exists y \forall x (x \in y \Leftrightarrow x \subseteq a)$

Схема издвајања. За произвољне скупове $a, a_1, \ldots, a_n$ и формулу $\varphi(x, a, a_1, \ldots, a_n)$ постоји скуп y који садржи само оне елементе x из a за које важи $\varphi(x, a, a_1, \ldots, a_n)$:

$\forall a \forall a_1 \cdots \forall a_n \exists y \forall x (x \in y \Leftrightarrow x \in a \wedge \varphi(x, a, a_1, \ldots, a_n))$

Аксиома регуларности. Сваки непразан скуп садржи елемент са којим нема заједничких елемената.

$\forall X (X \neq \emptyset \Rightarrow \exists x (x \in X \wedge x \cap X = \emptyset))$

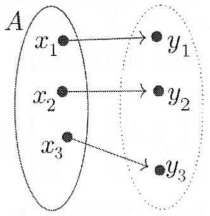
Аксиома бесконачности. Постоји скуп који садржи $\emptyset$ и следбеника сваког свог елемента. (Следбеник скупа x јесте скуп $x \cup \{x\}$.)

$\exists I (\emptyset \in I \wedge \forall x (x \in I \Rightarrow x \cup \{x\} \in I))$

Схема замене. За сваку формулу $\varphi(x, y)$,

$\forall x \exists ! y \varphi(x, y) \Rightarrow \forall A \exists B \forall y (y \in B \Leftrightarrow \exists x (x \in A \wedge \varphi(x, y)))$.

$\forall x \exists ! \, y \; \varphi(x, y)$



План

- аксиома замене
- аксиома регуларности
- аксиома бесконачности, индуктивни скупови
- природни бројеви: принцип математичке индукције, уређење природних бројева и принцип потпуне индукције, теорема рекурзије и основне рачунске операције

▼ Схема замене

Важан метод дефинисања функција омогућава нам нова схема – **схема замене**. Пре него што је наведемо, описаћемо ситуације у којима је користимо. Претпоставимо да смо, за неку формулу $\varphi(x,y)$, доказали $\forall x\exists! y\varphi(x,y)$. Ако је A било који скуп, тада мора да важи и $(\forall x\in A)\exists! y\varphi(x,y)$, што значи да за сваки x из A постоји јединствен y за који је $\varphi(x,y)$. Све ово указује на могућност да се формулом φ дефинише једна функција са доменом A. Међутим, да би на овај начин била дефинисана функција, неопходно је да знамо у ком скупу се налазе те јединствене „слике" елемената из A. Схема замене нас ослобађа сваке бриге по овом питању, јер тврди да за сваку формулу $\varphi(x,y)$ за коју се може утврдити $\forall x\exists! y\varphi(x,y)$ и сваки скуп A постоји скуп који садржи само оне скупове y за које $(\exists x\in A)\varphi(x,y)$.

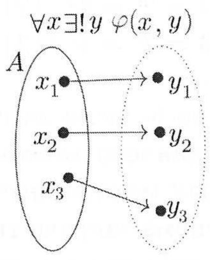


СХЕМА ЗАМЕНЕ

$$\forall x\exists! y\varphi(x,y)\Rightarrow \forall A\exists B\forall y(y\in B\Leftrightarrow \exists x(x\in A\wedge\varphi(x,y)))$$

▼ Аксиома регуларности

Аксиомом регуларности се тврди да сваки непразан скуп садржи елемент са којим нема заједничких елемената.

АКСИОМА РЕГУЛАРНОСТИ

$$\forall X(X\neq\emptyset\Rightarrow\exists x(x\in X\wedge x\cap X=\emptyset))$$

Теорема 23. *(1) Не постоји скуп x такав да $x\in x$.*
(2) Не постоје скупови x и y такви да $x\in y$ и $y\in x$.

ДОКАЗ. (1) Ако би постојао скуп x такав да $x\in x$, онда скуп $\{x\}$ не би садржао елемент са којим нема заједничких елемената, јер $x\in x\cap\{x\}$, што је супротно аксиоми регуларности.
(2) Претпоставимо да постоје скупови x и y такви да је $x\in y$ и $y\in x$. Тада, супротно аксиоми регуларности, скуп $\{x,y\}$ не садржи елемент са којим нема заједничких елемената: $x\cap\{x,y\}\neq\emptyset$, јер $y\in x\cap\{x,y\}$, и $y\cap\{x,y\}\neq\emptyset$, јер $x\in y\cap\{x,y\}$. □

Теорема 24. *За било које скупове x и y, из $x\cup\{x\}=y\cup\{y\}$ следи $x=y$.*

ДОКАЗ. Нека је $x\cup\{x\}=y\cup\{y\}$. Претпоставимо супротно ономе што треба доказати да је $x\neq y$. Како $x\in y\cup\{y\}$ и $x\neq y$, закључујемо да $x\in y$. Слично томе, из $y\in x\cup\{x\}$ и $x\neq y$ следи $y\in x$. Међутим, није могуће да $x\in y$ и $y\in x$, према претходној теореми (2). Дакле, $x=y$. □

Скуп $x\cup\{x\}$ називамо **следбеник** скупа x и обележавамо га x'. Полазећи од празног скупа, редом уводимо *следбенике* добијених скупова које из разумљивих разлога можемо идентификовати са природним бројевима:

$$
\begin{aligned}
0 = \emptyset \quad & 1 = 0' = \emptyset \cup \{\emptyset\} = \{0\} \\
& 2 = 1' = 1 \cup \{1\} = \{0\} \cup \{1\} = \{0, 1\} \\
& 3 = 2' = 2 \cup \{2\} = \{0, 1\} \cup \{2\} = \{0, 1, 2\} \\
& 4 = 3' = 3 \cup \{3\} = \{0, 1, 2\} \cup \{3\} = \{0, 1, 2, 3\} \\
& \dots
\end{aligned}
$$

Интуитивно је јасно да генерисање нових скупова на описани начин неограничено можемо продужавати – за сваки добијени скуп, поступак можемо наставити увођењем његовог следбеника. Наредна аксиома заправо тврди да постоји скуп у коме ће се наћи сви скупови који се могу добити на описани начин. Будући да је описани поступак веома близак *бројању*, наредна аксиома ће бити кључна за увођење скупа природних бројева.

▼ Аксиома бесконачности. Скуп природних бројева

> Аксиома бесконачности
> Постоји скуп који садржи 0 (тј. $\emptyset$) и следбеника сваког свог елемента.
> $$\exists I (0 \in I \wedge \forall x (x \in I \Rightarrow x \cup \{x\} \in I))$$

Сваки скуп који садржи 0 и следбеника сваког свог елемента називамо **индуктивним скупом**. Аксиомом бесконачности се тврди да постоји бар један индуктиван скуп. Не можемо тврдити да постоји јединствен индуктиван скуп, али колико год да их има сви садрже као подскуп један исти индуктиван скуп, тзв. *најмањи индуктиван скуп*.

Ако је I неки индуктиван скуп, означимо са $\mathcal{I}(I)$ непразан скуп свих индуктивних подскупова од I:

$$
\begin{aligned}
\mathcal{I}(I) &= \{X \mid X \subseteq I \wedge \text{„}X \text{ је индуктиван"}\} \\
&= \{X \mid X \subseteq I \wedge 0 \in X \wedge \forall x (x \in X \Rightarrow x' \in X)\}.
\end{aligned}
$$

Нека је $\omega \stackrel{\text{def}}{=} \bigcap \mathcal{I}(I)$. Доказаћемо да је ω индуктиван скуп и то најмањи у следећем смислу: ако је S индуктиван и $S \subseteq \omega$, онда је $S = \omega$, односно не постоји строги подскуп од ω који је индуктиван.

Теорема 25. *(1) ω је индуктиван скуп.*
(2) Ако је $S \subseteq \omega$ и важи:

(БИ) $0 \in S$,

(ИК) ако $x \in S$, онда $x' \in S$,

онда је $S = \omega$

Доказ. (1) Будући да за сваки $X \in \mathcal{I}(I)$, $0 \in X$, следи да мора бити и $0 \in \bigcap \mathcal{I}(I) = \omega$.

Остаје још да се покаже да ω садржи следбеника сваког свог елемента. Нека је $x \in \omega$ произвољан. Из $x \in \omega = \bigcap \mathcal{I}(I)$, следи да $x \in X$, за сваки $X \in \mathcal{I}(I)$. Како је сваки $X \in \mathcal{I}(I)$ индуктиван, сваки од њих садржи и x'. Дакле, $x' \in \bigcap \mathcal{I}(I) = \omega$.

(2) Нека је $S \subseteq \omega$ такав да важе услови (БИ) и (ИК) – значи S је индуктиван подскуп од ω. Како је $\omega \subseteq I$, скуп S је и индуктиван подскуп од I, тј. $S \in \mathcal{I}(I)$, па је $\bigcap \mathcal{I}(I) \subseteq S$, тј. $\omega \subseteq S$, одакле следи да је $S = \omega$. □

Остаје још да покажемо да за било који (други) индуктиван скуп I_1 важи $\omega \subseteq I_1$, или еквивалентно $\omega \cap I_1 = \omega$. Очигледно је $\omega \cap I_1 \subseteq \omega$. Једноставно је уверити се да скуп $\omega \cap I_1$ задовољава услове (БИ) и (ИК), па према претходној теореми (2) мора бити $\omega \cap I_1 = \omega$. Одавде непосредно закључујемо и да је $\omega = \bigcap \mathcal{I}(I_1)$. Скуп ω називамо **скупом природних бројева** и обележавамо га и $\mathbb{N}$. Будући да је ова друга ознака много уобичајенија, углавном ћемо њу користити у наставку. Знамо да $\mathbb{N}$ садржи 0, 1, 2, 3, 4, итд. и да функција *следбеник* $'$: $\mathbb{N} \to \mathbb{N}$ има следеће особине:

- за свако $n \in \mathbb{N}$, $n' \neq 0$ (следбеник није на функција);
- за све $m, n \in \mathbb{N}$, из $m' = n'$ следи $m = n$ (следбеник јесте 1-1 функција).

Основно својство скупа природних бројева изражено је особином (2) теореме 25 – **принципом математичке индукције**.[128] Неколико начина примене овог принципа илуструјемо доказивањем следећих важних тврђења.

[128] Принцип математичке индукције користимо за доказивање формула облика $(\forall n \in \mathbb{N})\, \varphi(n)$. Прво формирамо одговарајући скуп $S = \{n \in \mathbb{N} \mid \varphi(n)\}$ и настојимо да докажемо:

(БИ) *базу индукције*, тј. $0 \in S$ и

(ИК) *индуктивни корак*, тј. да из $n \in S$ следи $n' \in S$. Пошто у индуктивном кораку треба доказати импликацију, претпостављамо $n \in S$, што се назива *индуктивна претпоставка* и настојимо да докажемо $n' \in S$.

Доказ применом принципа математичке индукције можемо скратити тако што не формирамо скуп S већ доказујемо формуле:

(БИ) $\varphi(n/0)$

(ИК) $(\forall n \in \mathbb{N})(\varphi \Rightarrow \varphi(n/n'))$.

Теорема 26. *(1) За све природне бројеве m, n, $m \in n \Rightarrow m \subseteq n$.*
(2) За све природне бројеве m, n, $m \in n \Leftrightarrow m \subset n$.
(3) За све природне бројеве m, n, $m \in n \vee m = n \vee n \in m$.

Доказ. (1) Да бисмо доказали

$$(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n),$$

формирамо скуп

$$S = \{n \in \mathbb{N} \mid (\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n)\}$$

и доказујемо да је $S = \mathbb{N}$, применом принципа математичке индукције.

(БИ) Докажимо да $0 \in S$, тј. $(\forall m \in \mathbb{N})(m \in 0 \Rightarrow m \subseteq 0)$. Како је $0 = \emptyset$ и знамо да за свако m важи $m \notin 0$, онда се из претпоставке $m \in 0$ изводи било шта ($\bot_{\mathrm{E}}$), па и $m \subseteq 0$. Дакле, $0 \in S$.

(ИК) Претпоставимо да $n \in S$, тј.

(ИП) $$(\forall m \in \mathbb{N})(m \in n \Rightarrow m \subseteq n).$$

Треба да докажемо $n' \in S$, тј. $(\forall m \in \mathbb{N})(m \in n' \Rightarrow m \subseteq n')$. Из $m \in n' = n \cup \{n\}$ следи да $m \in n$ или $m = n$. У случају да је $m \in n$, према (ИП) закључујемо $m \subseteq n$, па је $m \subseteq n \cup \{n\} = n'$. У случају $m = n$, непосредно закључујемо да $m = n \subseteq n'$.

Дакле, $S = \mathbb{N}$.

(2) И у овом случају користимо принцип математичке индукције, али ћемо поступити мало другачије у односу на доказ тврђења (1).

Нека је m произвољан природан број и

$$S_m = \{n \in \mathbb{N} \mid m \in n \Leftrightarrow m \subset n\}.$$

Доказаћемо да је $S_m = \mathbb{N}$.[129]

(БИ) Знамо да $m \notin 0$ и $m \not\subset 0$ (празан скуп нема праве подскупове), одакле једноставно изводимо $m \in 0 \Leftrightarrow m \subset 0$. Дакле, $0 \in S_m$.

(ИК) Претпоставимо да $n \in S_m$, тј. (ИП) $m \in n \Leftrightarrow m \subset n$.

Докажимо $m \in n' \Leftrightarrow m \subset n'$.

Ако $m \in n' = n \cup \{n\}$, онда $m \in n$ или $m = n$. У случају да $m \in n$, према (ИП) следи $m \subset n$, а тиме и $m \subset n'$, јер је $n \subset n'$. У случају да је $m = n$, онда је очигледно $m \subset n'$.

Нека је $m \subset n' = n \cup \{n\}$. Докажимо најпре да $n \notin m$. Ако би било $n \in m$, имали бисмо $\{n\} \subseteq m$ и, према (1), $n \subseteq m$, одакле следи $n' = n \cup \{n\} \subseteq m \subset n'$, што је немогуће. Дакле, $n \notin m$, па из $m \subset n \cup \{n\}$, следи $m \subseteq n$, тј. $m \subset n$ или $m = n$. У случају да је $m \subset n$, према (ИП) закључујемо да $m \in n$, а самим тим и $m \in n'$. У случају да је $m = n$, директно добијамо $m = n \in n'$.

Дакле, $S_m = \mathbb{N}$ за сваки природан број m, одакле следи жељено тврђење.

(3) Нека је $S = \{m \in \mathbb{N} \mid (\forall n \in \mathbb{N})(m \in n \vee m = n \vee n \in m)\}$.

(БИ) Докажимо $(\forall n \in \mathbb{N})(0 \in n \vee 0 = n \vee n \in 0)$.

Очигледно је да за било које $n \in \mathbb{N}$ важи $n = 0$ или $n \neq 0$. У случају $n = 0$, директно изводимо $0 \in n \vee 0 = n \vee n \in 0$. Уколико је $n \neq 0$, тада је $\emptyset = 0 \subset n$, па према тврђењу (2) закључујемо $0 \in n$, а тиме и $0 \in n \vee 0 = n \vee n \in 0$. Дакле, $0 \in S$.

(ИК) Претпоставимо да $m \in S$, тј.

(ИП) $(\forall n \in \mathbb{N})(m \in n \vee m = n \vee n \in m)$.

Да бисмо доказали

$$(*) \qquad (\forall n \in \mathbb{N})(m' \in n \vee m' = n \vee n \in m'),$$

изаберимо произвољан $n \in \mathbb{N}$. Тада према (ИП) важи $m \in n$ или $m = n$ или $n \in m$. Разликујемо три случаја.

1. случај: $m \in n$. Тада је, према (2), $m \subset n$, па је $m' = m \cup \{m\} \subseteq n$. Уколико је $m' \subset n$, онда, поново према (2), важи $m' \in n$, па самим тим важи $(*)$. Формула $(*)$ свакако важи и уколико је $m' = n$.

2. случај: $m = n$. Тврђење $(*)$ важи јер $n \in n' = m'$.

3. случај: $n \in m$. Непосредно добијамо $n \in m'$, па важи $(*)$. □

▼ Уређење и аритметичке операције скупа $\mathbb{N}$

Претходна теорема показује да припадање ($\in$), односно строга инклузија ($\subset$) на уобичајени начин уређују скуп природних бројева:

$$0 \in 1 \in 2 \in 3 \in 4 \in 5 \cdots, \quad \text{односно} \quad 0 \subset 1 \subset 2 \subset 3 \subset 4 \subset 5 \cdots$$

Заиста, знамо да:

[129] Уколико треба доказати формулу облика

(Φ) $$(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})\varphi(m,n),$$

због еквивалентности ове формуле са $(\forall n \in \mathbb{N})(\forall m \in \mathbb{N})\varphi(m,n)$, можемо поступити двојако:

1) За било који, произвољно изабран број $m \in \mathbb{N}$, формирамо скуп $S_m = \{n \in \mathbb{N} \mid \varphi(m,n)\}$ и индукцијом доказујемо $S_m = \mathbb{N}$. Када успемо, изводимо закључак $(\forall m \in \mathbb{N})\, S_m = \mathbb{N}$.

2) За било који, произвољно изабран број $n \in \mathbb{N}$, формирамо скуп $S_n = \{m \in \mathbb{N} \mid \varphi(m,n)\}$ и индукцијом доказујемо $S_n = \mathbb{N}$. Када успемо, изводимо закључак $(\forall n \in \mathbb{N})\, S_n = \mathbb{N}$.

У сваком од наведених случајева непосредно следи (Φ). У првом случају (Φ) доказујемо *индукцијом по n при фиксираном m*, а у другом случају *индукцијом по m при фиксираном n*.

- за сваки природан број n важи $n \notin n$ (ово је последица аксиоме регуларности – теорема 23 (1), али се може извести и без ове аксиоме, математичком индукцијом);
- за све природне бројеве k, m, n, ако $k \in m$ и $m \in n$, онда $k \in n$ (ово је директна последица претходне теореме (2)).

Дакле, бинарна релација $\{(m,n) \in \mathbb{N} \times \mathbb{N} \mid m \in n\}$ јесте *строго уређење скупа природних бројева* и обележава се $<$. Релацију $\leqslant$, тзв. *уређење* скупа $\mathbb{N}$ уводимо на следећи начин:

$$m \leqslant n \overset{\text{def}}{\Leftrightarrow} m < n \vee m = n.$$

Последица 3. *За све природне бројеве m, n важи*[130]
(1) $m \leqslant n \Leftrightarrow m \subseteq n$;
(2) $m \leqslant n \vee n \leqslant m$ (поредак $\leqslant$ је линеаран);
(3) $m < n \Leftrightarrow m' \leqslant n$;
(4) $m < n' \Leftrightarrow m \leqslant n$;
(5) $m < n \Leftrightarrow m' < n'$ (функција следбеник је монотона).

Доказ. (1) Према претходној теореми (2) имамо да је:

$$m \leqslant n \Leftrightarrow m < n \vee m = n \Leftrightarrow m \subset n \vee m = n \Leftrightarrow m \subseteq n.$$

(2) Директно из тврђења (3) претходне теореме.
(3) Ако је $m < n$, тј. $m \in n$, онда је $\{m\} \subseteq n$ и, према теореми 26 (1), $m \subseteq n$, па је $m' = m \cup \{m\} \subseteq n$, тј. $m' \leqslant n$.

Из $m' \leqslant n$ следи $m' < n$ или $m' = n$, и у оба случаја, будући да је $m < m'$, закључујемо $m < n$.
(4) и (5) Доказе остављамо за вежбу. □

[130] Наравно, $\leqslant$ наслеђује основна својства инклузије $\subseteq$. За све $k, m, n \in \mathbb{N}$:

- $n \leqslant n$;
- $m \leqslant n \wedge n \leqslant m \Rightarrow m = n$;
- $k \leqslant m \wedge m \leqslant n \Rightarrow k \leqslant n$.

Теорема 27. [***Принцип потпуне индукције***] *Нека је $S \subseteq \mathbb{N}$. Ако важи*

$$(\forall n \in \mathbb{N})((\forall k < n)\, k \in S \Rightarrow n \in S),$$

онда је $S = \mathbb{N}$.

Доказ. [131] Формулу $(\forall k < n)\, k \in S$ можемо записати и на следећи начин: $(\forall k \in n)\, k \in S$.

Приметимо најпре да важи

(БИ) $$(\forall k < 0)\, k \in S.$$

Ова формула је заправо скраћење за $\forall k\, (k \in 0 \Rightarrow k \in S)$ и једноставно се доказује, јер знамо да за свако k важи $k \notin 0$.

Није тешко уочити, а ни формално доказати, да је формула

$$(\forall k < n)\, k \in S \Rightarrow n \in S$$

еквивалентна формули

(ИК) $$(\forall k < n)\, k \in S \Rightarrow (\forall k < n')\, k \in S.$$

Из (БИ) и (ИК), према принципу математичке индукције, следи

$$(\forall n \in \mathbb{N})(\forall k < n)\, k \in S.$$

Најзад, из последње формуле и претпоставке $S \subseteq \mathbb{N}$ закључујемо $S = \mathbb{N}$. □

[131] Уопштено говорећи, „обичном" индукцијом (по n) доказујемо формулу

$$(\forall k < n) k \in S.$$

Из $(\forall n \in \mathbb{N})(\forall k < n) k \in S$ следи $S = \mathbb{N}$.

Теорема 28. *Сваки непразан подскуп скупа природних бројева има најмањи елемент.*

Доказ. Нека је X подскуп од $\mathbb{N}$ који нема најмањи елемент. Доказаћемо да X мора бити празан, тј. да је $\mathbb{N} \setminus X = \mathbb{N}$. Ову једнакост доказујемо применом принципа потпуне индукције.

Нека је n природан број такав да је $(\forall k < n)\, k \in \mathbb{N} \setminus X$. Ако би број n припадао X, онда би он био најмањи елемент скупа X, јер сваки k мањи од n припада $\mathbb{N} \setminus X$. Дакле, $n \in \mathbb{N} \setminus X$. Према принципу потпуне индукције закључујемо $\mathbb{N} \setminus X = \mathbb{N}$, односно $X = \varnothing$. □

Принцип потпуне индукције заправо тврди да за сваки $S \subseteq \mathbb{N}$ важи:

$$(\forall n \in \mathbb{N})((\forall k < n)\, k \in S \Rightarrow n \in S) \Rightarrow (\forall n \in \mathbb{N})\, n \in S.$$

Наравно, за сваки $S \subseteq \mathbb{N}$ важи и

$$(\forall n \in \mathbb{N})((\forall k < n)\, k \in S^{\complement} \Rightarrow n \in S^{\complement}) \Rightarrow (\forall n \in \mathbb{N})\, n \in S^{\complement},$$

одн. применом закона контрапозиције:

$$\neg(\forall n \in \mathbb{N})\, n \in S^{\complement} \Rightarrow \neg(\forall n \in \mathbb{N})((\forall k < n)\, k \in S^{\complement} \Rightarrow n \in S^{\complement}).$$

Последња формула се једноставно трансформише у еквивалентну формулу

$$\underbrace{(\exists n \in \mathbb{N})\, n \in S}_{S \text{ је непразан}} \Rightarrow \underbrace{(\exists n \in \mathbb{N})((\forall k < n)\, k \notin S \wedge n \in S)}_{S \text{ има најмањи елемент}},$$

којом се тврди да *сваки непразан подскуп од* $\mathbb{N}$ *има најмањи елемент.*

Дефиниција 22. *Уређење* $\leqslant$ *неког скупа* X *је* ***добро*** *ако сваки непразан подскуп од* X *има најмањи елемент у односу на* $\leqslant$.

Истичемо да је свако добро уређење такође линеарно. Заиста, за свака два елемента x и y доброг уређења, подскуп $\{x, y\}$ има најмањи елемент, па мора бити $x \leqslant y$ или $y \leqslant x$. Наравно, обратно није тачно у општем случају: линеарно уређење не мора бити добро.

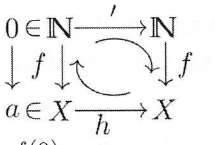
Дакле, скуп природних бројева је добро уређен скуп.

▼ Теорема рекурзије. Основне аритметичке операције

Теорема рекурзије омогућава да дефинишемо функције чији је домен $\mathbb{N}$, на начин који потпуно одговара „природи” скупа $\mathbb{N}$.

Теорема 29. [***Принцип рекурзије***] *Нека је* X *неки скуп,* $g \in X$ *и* $h : X \to X$. *Тада постоји јединствена функција* $f : \mathbb{N} \to X$ *таква да је*

$$(\text{Rec}) \left|\; \begin{array}{l} f(0) = g, \\ f(n') = h(f(n)),\ n \in \mathbb{N}. \end{array}\right.$$



$f(0) = g$
$f \circ {}'(n) = h \circ f(n)$

Доказ. **Егзистенција.**

Скуп $F \subseteq \mathbb{N} \times X$ назваћемо (g, h)-скупом ако су задовољени следећи услови:

1) $(0, g) \in F$ и

2) за све $n \in \mathbb{N}$ и $x \in X$, ако $(n, x) \in F$, онда и $(n', h(x)) \in F$.

Очигледно је $\mathbb{N}\times X$ један (g,h)-скуп, па је непразна колекција $\mathcal{F}$ свих (g,h)-скупова. Нека је $f=\bigcap\mathcal{F}$. Тада је $f\subseteq\mathbb{N}\times X$. Доказаћемо да је f заправо тражена функција.Доказ ове чињенице је дугачак само зато што ћемо неколико пута проверавати услове 1) и 2), тј. доказивати да је неки скуп заиста (g,h)-скуп.

Подсећамо: f је функција из A у B, у ознаци $f:A\to B$, ако је $f\subseteq A\times B$ и за свако $a\in A$ постоји јединствено $b\in B$ тако да је $(a,b)\in f$.

Докажимо најпре да је $f=\bigcap\mathcal{F}$ један (g,h)-скуп.

1) За свако $F\in\mathcal{F}$, $(0,g)\in F$, одакле следи да $(0,g)\in\bigcap\mathcal{F}=f$.

2) Претпоставимо да $(n,x)\in f=\bigcap\mathcal{F}$. Тада за свако $F\in\mathcal{F}$, $(n,x)\in F$, па и $(n',h(x))\in F$ (јер F (g,h)-скуп). Дакле, $(n',h(x))\in\bigcap\mathcal{F}=f$.

Даље, доказујемо да је f функција из $\mathbb{N}$ у X, одн. да за свако $k\in\mathbb{N}$ постоји јединствено $y\in X$ тако да $(k,y)\in f$.

(БИ) Доказујемо базу индукције ($k=0$). Како је f један (g,h)-скуп, знамо да $(0,g)\in f$. Претпоставимо да постоји још једно $g_1\in X$ такво да $(0,g_1)\in f$ и $g\neq g_1$. Нека је $f_1=f\setminus\{(0,g_1)\}$. Докажимо да је f_1 један (g,h)-скуп.

1) $(0,g)\in f_1$, јер је из f избачен само елемент $(0,g_1)$ и $g_1\neq g$.

2) Претпоставимо да за неке $n\in\mathbb{N}$ и $x\in X$, $(n,x)\in f_1$. Будући да тада $(n,x)\in f$ имамо и да $(n',h(x))\in f$. Како је $(n',h(x))\neq(0,g_1)$, јер је $0\neq n'$, следи да $(n',h(x))\in f_1$.

Дакле, $f'\in\mathcal{F}$, па је $f=\bigcap\mathcal{F}\subsetneqq f_1$, што је контрадикција.

(ИК) Доказујемо индуктивни корак.

(ИП) Претпоставимо да за $k\in\mathbb{N}$ постоји тачно један $y\in X$ такав да је $(k,y)\in f$.

Пошто је f један (g,h)-скуп, имамо да $(k',h(y))\in f$. Претпоставимо да постоји и $y_1\in X$ такав да $(k',y_1)\in f$ и $y_1\neq h(y)$. Нека је $f_1=f\setminus\{(k',y_1)\}$. Докажимо да је f_1 један (g,h)-скуп.

1) $(0,g)\in f'$, јер је из f избачен само елемент (k',y_1) који је сигурно различит од $(0,g)$, будући да је $0\neq k'$.

2) Претпоставимо да $(n,x)\in f_1$, за неке $n\in\mathbb{N}$ и $x\in X$. Из $(n,x)\in f$ следи $(n',h(x))\in f$. Докажимо да је $(n',h(x))\neq(k',y_1)$. Неједнакост је очигледно тачна ако је $n'\neq k'$. Ако је $n'=k'$, онда је и $n=k$, па је $x=y$ (јер је y једини елемент из X такав да $(k,y)\in f$). Према избору елемента y_1 имамо да је $y_1\neq h(y)=h(x)$, одакле следи $(n',h(x))\neq(k',y_1)$.

Дакле, $f=\bigcap\mathcal{F}\subsetneqq f'$, што је контрадикција.

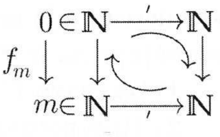
Доказ математичком индукцијом је завршен; доказали смо да је f функција из $\mathbb{N}$ у X. Ова функција задовољава једнакости (Rec), јер је f (g,h)-скуп:

- Из услова 1) произлази $f(0)=g$;
- Према услову 2), из $f(n)=x$ следи да је $f(n')=h(x)$, тј. $f(n')=h(f(n))$.

Јединственост.

Претпоставимо да функције $f_1,f_2:\mathbb{N}\to X$ задовољавају једнакости (Rec). Доказаћемо да су оне једнаке, тј. да за свако $n\in\mathbb{N}$ важи $f_1(n)=f_2(n)$. Доказ изводимо математичком индукцијом.

(БИ) $f_1(0) = g = f_2(0)$
(ИК) Претпоставимо да за неко $n \in \mathbb{N}$ важи $f_1(n) = f_2(n)$. Тада је $f_1(n') = h(f_1(n)) = h(f_2(n)) = f_2(n')$. □



Користећи претходну теорему, уводимо основне аритметичке операције. Ако је $m \in \mathbb{N}$ неки фиксирани природан број, према теореми рекурзије, постоји јединствена функција $f_m : \mathbb{N} \to \mathbb{N}$, таква да је:

$$f_m(0) = m$$
$$f_m(n') = f_m(n)'$$

Уместо $f_m(n)$ пишемо $m + n$. Уз овакво означавање, горње једнакости постају:

$$m + 0 = m$$
$$m + n' = (m + n)'$$

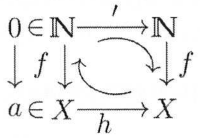
Није тешко уочити да је $n' = n + 1$, за сваки природан број n.

Аналогно се уводе *множење* и *степеновање*:

$$\left|\begin{array}{l} m \cdot 0 = 0, \\ m \cdot n' = m + (m \cdot n). \end{array}\right. \qquad \left|\begin{array}{l} m^0 = 1, \\ m^{n+1} = m \cdot m^n. \end{array}\right.$$

Сва позната својства ових операција и њихове везе са уређењем доказујемо математичком индукцијом (видети задатке 6 и 10, на страни 125).

Скуп природних бројева $\mathbb{N}$ је суштински одређен својим (почетним) елементом 0 и функцијом (следбеник) $' : \mathbb{N} \to \mathbb{N}$. Теорема рекурзије тврди да за било који скуп X, изабрани елемент $a \in X$ и функцију $h : X \to X$, једнакости (Rec) одређују јединствену функцију $f : \mathbb{N} \to X$.



$$f(0) = a$$
$$f(n') = h(f(n)), \text{ тј. } f \circ {}' (n) = h \circ f\,(n)$$

Уколико је X неки скуп, свака функција из $\mathbb{N}$ у X назива се и **низ** у скупу X. Низови су веома важни у свим областима математике, па се усвајају разни договори о ознакама. Аргумент функције (низа) $f : \mathbb{N} \to X$ често се записује као индекс слова којим је функција означена: уместо $f(n)$ пише се f_n. У складу са тим, некада се уместо „$f : \mathbb{N} \to X$" пише „$(f_n)_{n \in \mathbb{N}}$". Поред тога, како је $n' = n + 1$, уз претходне договоре, теорема рекурзије тврди да за изабране $a \in X$ и $h : X \to X$, постоји јединствени низ $(f_n)_{n \in \mathbb{N}}$ одређен једнакостима:

$$(\text{Rec}) \begin{cases} f_0 = a, \\ f_{n+1} = h(f_n),\ n \in \mathbb{N}. \end{cases}$$

За низ одређен једнакостима (Rec) кажемо да је **рекурзивно** (рекурентно, индуктивно) дефинисан.

▼ Задаци и додаци

1. Аксиома пара се може извести из осталих акиома теорије **ZF**. Доказ те чињенице растављамо на неколико основних корака садржаних у наредним захтевима:
(а) Оправдати конструкцију скупа $\{\varnothing, \{\varnothing\}\}$, користећи аксиоме теорије **ZF**, без аксиоме пара.
(б) За произвољне a и b, нека је $\varphi(x, y)$ формула

$$(x = \varnothing \wedge y = a) \vee (x \neq \varnothing \wedge y = b).$$

Доказати $\forall x \exists! y\, \varphi(x, y)$.
(в) За произвољне a и b објаснити конструкцију скупа $\{a, b\}$ применом схеме замене за скуп $\{\varnothing, \{\varnothing\}\}$, користећи формулу $\varphi(x, y)$.
2. Доказати да не постоје скупове x, y и z такви да $x \in y$, $y \in z$ и $z \in x$.
3. Да ли постоји скуп x такав да $\{x\} \in x$? Да ли постоји скуп x такав да је $\{x\} \subseteq x$? Образложити одговоре.
4. Ако је могуће, навести пример скупа чији је сваки елемент уједно и подскуп тог скупа.
5. Нека је $f : \mathbb{N} \to \mathbb{N}$ функција која комутира са функцијом следбеник, тј. $f(n+1) = f(n) + 1$, за све $n \in \mathbb{N}$. Доказати да је $f(n+1) = n + f(1)$, за све $n \in \mathbb{N}$.
6. Доказати да за било које природне бројеве k, m, n важи:
(а) $m + n = n + m$ (сабирање је комутативно);
(б) $k + (m + n) = (k + m) + n$ (сабирање је асоцијативно);
(в) $m \cdot 1 = m$ (неутрал за множење је 1);
(г) $m \cdot n = n \cdot m$ (множење је комутативно);
(д) $k \cdot (m \cdot n) = (k \cdot m) \cdot n$ (множење је асоцијативно);
(ђ) $k \cdot (m + n) = k \cdot m + k \cdot n$ (леви закон дистрибутивности);
(е) $1^m = 1$;
(ж) $m^1 = m$;
(з) $k^{m+n} = k^m \cdot k^n$;
(и) $(k \cdot m)^n = k^n \cdot m^n$;
(ј) $(k^m)^n = k^{m \cdot n}$.
7. Доказати да за свако $m \in \mathbb{N} \setminus \{0\}$ постоји $n \in \mathbb{N}$ тако да је $m = n'$.
8. Доказати да за све $m, n \in \mathbb{N}$ важи:
(а) $m + n = 0 \Leftrightarrow m = 0 \wedge n = 0$
(б) $m + n = 1 \Leftrightarrow (m = 1 \wedge n = 0) \vee (m = 0 \wedge n = 1)$
(в) $m \cdot n = 0 \Leftrightarrow m = 0 \vee n = 0$
(г) $m \cdot n = 1 \Leftrightarrow m = 1 \wedge n = 1$
9. Доказати да за све $m, n \in \mathbb{N}$ важи:
(а) $m \leqslant m + n$
(б) $m \leqslant n \Leftrightarrow (\exists k \in \mathbb{N})\, n = m + k$
10. Доказати да за све $k, m, n \in \mathbb{N}$ важи:
(а) $k = m \Leftrightarrow k + n = m + n$
(б) $n = m + n \Leftrightarrow m = 0$

(в) $k < m \Leftrightarrow k + n < m + n$

(г) $n < m + n \Leftrightarrow 0 < m$

11. Доказати да за све $k, m, n \in \mathbb{N}$ важи:

(а) $0 < k \wedge m < n \Rightarrow k \cdot m < k \cdot n$

(б) $0 < k \wedge k \cdot m = k \cdot n \Rightarrow m = n$

(в) $0 < k \wedge k \cdot m < k \cdot n \Rightarrow m < n$

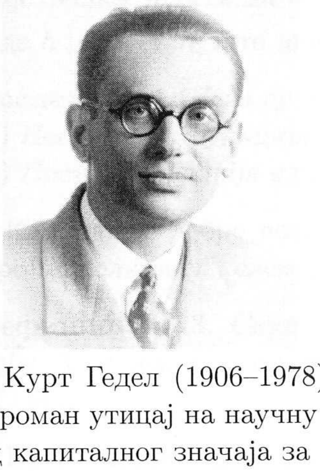
12. Нека $g : S \to X$ и $h : S \times X \to X$. Доказати да постоји јединствена функција $f : S \times \mathbb{N} \to X$ таква да за свако $s \in S$:

$$(\mathrm{Rec}) \left| \begin{array}{l} f(s,0) = g(s), \\ f(s,n') = h(s, f(s,n)),\ n \in \mathbb{N}. \end{array} \right.$$

4. Заснивање математике

Да би се размишљало продуктивно, морају се користити све интуитивне и неформалне методе расуђивања које су на располагању.

Пол Коен (1934–2007), цитат из чланка *Откриће форсинга* (The discovery of Forcing), објављеног 2002. године, у коме описује своју револуционарну методу доказивања независности неких тврдњи од аксиома теорије скупова



Курт Гедел (1906–1978) био је аустријско-амерички математичар и филозоф који је имао огроман утицај на научну и филозофску мисао 20. века. Скоро сви Геделови резултати су били од капиталног значаја за разне области математичке логике: теорију доказа, теорију скупова, теорију израчунљивости (а самим тим и теоријско рачунарство) итд.

4.1. **Кардиналност скупа**

Увод. Да ли међу бројевима $0, 1, 2, 3, \ldots, 999$ има више оних са збиром цифара 10 или оних са збиром цифара 17?

Означимо са A скуп свих бројева мањих од 1000 чији је збир цифара једнак 10, а са B скуп свих бројева мањих од 1000 чији је збир цифара једнак 17.

Пописивање и бројање елемената сваког скупа јесте један начин да одговоримо на постављено питање. Постоји много довитљивији начин да се одговори на питање.

Сваки од бројева $0, 1, 2, \ldots, 999$ можемо посматрати као 'реч' облика abc, где су a, b, c неке од цифара $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, при чему речи које одговарају једноцифреним и двоцифреним бројевима добијамо дописивањем нула испред броја; на пример, броју 9 одговара реч 009, а броју 10 реч 010. Скупове A и B сада посматрамо као скупове одговарајућих троцифрених речи.

Дефинишимо функцију $f : A \to B$:

$$f(abc) = xyz \text{ где је } x = 9 - a, y = 9 - b, z = 9 - c.$$

На пример, $f(019) = 981$, $f(564) = 435$, итд. Није тешко уочити да ако $abc \in A$, тј. ако је $a + b + c = 10$, тада $f(abc) \in B$. Заиста, ако је $f(abc) = xyz$ и $a + b + c = 10$, онда је:

$$x + y + z = 9 - a + 9 - b + 9 - c = 27 - 10 = 17.$$

Функција f је бијекција.

- f је 1-1: ако је $abc \neq a'b'c'$, тада важи бар једна од неједнакости $a \neq a'$ или $b \neq b'$ или $c \neq c'$, па тиме и бар једна од неједнакости $9 - a \neq 9 - a'$, $9 - b \neq 9 - b'$, $9 - c \neq 9 - c'$, и сходно томе мора бити $f(abc) \neq f(a'b'c')$.
- f је на: за произвољну реч $xyz \in B$, нека је $a = 9 - x$, $b = 9 - y$, $c = 9 - z$, одакле очигледно следи да $abc \in A$ и $f(abc) = xyz$.

Успостављањем бијекције између скупова A и B показали смо да ова два скупа имају исти број елемената.

План

- Коначни скупови; Дирихлеов принцип
- Бесконачни скупови; Кантор-Бернштајнова теорема
- Пребројиви и непребројиви скупови; $|X| < |\mathcal{P}(X)|$

▼ Коначни скупови. Дирихлеов принцип

Један од основних комбинаторних принципа познат је под називом *принцип куглица и кутија* или *Дирихлеов принцип*:

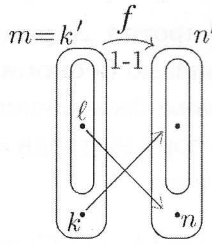
> Ако m куглица распоредимо у n кутија, при чему је $m > n$, онда се у бар једној кутији налазе бар две куглице; другим речима, распоређивање куглица не може бити 1-1 (једнозначно).

Густав Лежен Дирихле (1805–1859), немачки математичар

Теорема 30. [**Дирихлеов принцип**] *За свака два природна броја m и n, ако је $m > n$, онда не постоји 1-1 функција из m у n.*

Доказ. Доказ изводимо индукцијом по n.
(БИ) Ако је $m > 0$, тада уопште не постоји функција из m у 0 ($m \neq \emptyset$ и $0 = \emptyset$), па тврђење тривијално важи.
(ИК) (ИП) Нека је n природан број такав да за било које $m > n$ не постоји 1-1 функција из m у n. Доказаћемо да тада за свако $m > n'$, такође не постоји 1-1 функција из m у n'.

Претпоставимо супротно: нека је $m > n'$ и $f : m \overset{1-1}{\to} n'$. Одавде следи да n ($n \in n'$) мора бити f-слика неког елемента из m, јер би у супротном постојала 1-1 функција из m у n, што није могуће. Такође, из $m > n'$, следи да постоји природан број k такав да је $m = k'$; $f : k \cup \{k\} \overset{1-1}{\to} n \cup \{n\}$. Како је $k' > n'$, према последици 3 (5) (страна 121) имамо да је $k > n$, па не постоји 1-1 функција из k у n. Разликујемо два случаја: $f(k) = n$ и $f(k) \neq n$.
1. случај: $f(k) = n$. Тада $f\,|_k\colon k \overset{1-1}{\to} n$, што је немогуће према (ИП).
2. случај: $f(k) \neq n$. Тада је $f(\ell) = n$, за неко $\ell \in k$, тј. $\ell < k$. Дефинишимо функцију $h : k' \to n'$ на следећи начин:



$$h(x) = \begin{cases} f(x), & x \in k \wedge x \neq \ell \\ f(k), & x = \ell, \\ n, & x = k. \end{cases}$$

Није тешко уочити да $h : k' \overset{1-1}{\to} n'$ и да је $h(k) = n$. Међутим, тада $h\,|_k\colon k \overset{1-1}{\to} n$, што није могуће према (ИП). □

Последица 4. *Нека су m и n произвољни природни бројеви.*
(1) Постоји 1-1 функција из m у n ако и само ако је $m \leqslant n$.
(2) Постоји бијекција између m и n ако и само ако је $m = n$.

Као што је добро познато, природним бројевима изражавамо „број” („количину”) елемената коначних скупова.

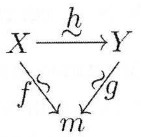
Дефиниција 23. *Скуп X је* **коначан** *ако постоји бијекција између X и неког природног броја n, и у том случају пишемо $|X| = n$.*

Према последици 4 (2), за сваки коначан скуп X постоји *јединствен* природан број n такав да је $|X| = n$ и тада кажемо да је n

број елемената скупа X, одн. *кардиналност* скупа X једнака је n. Очигледно је $|n| = n$ за било који природан број n.

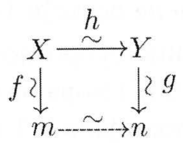
Теорема 31. *Нека су X и Y неки коначни скупови. Тада важи:*
(1) $|X| = 0 \Leftrightarrow X = \emptyset$;
(2) $|X| = |Y|$ ако и само ако постоји бијекција између X и Y.
(3) $|X| \leqslant |Y|$ ако само ако постоји 1-1 функција из X у Y.

Доказ. (1) Тврђење директно следи из разматрања о функцијама из празног и у празан скуп са стране 99.
(2) Будући да су X и Y коначни скупови, постоје природни бројеви m и n и бијекције $f : X \xrightarrow[\text{на}]{1-1} m$ и $g : Y \xrightarrow[\text{на}]{1-1} n$.



($\Rightarrow$) Претпоставимо да је $m = n$. Треба да дефинишемо бијекцију између X и Y. На наредној слици, знаком $\sim$ изнад стрелице означавамо да је одговарајућа функција бијекција.

Функција $h : X \to Y$, дата са $h(x) = g^{-1} \circ f(x)$, јесте бијекција.
($\Leftarrow$) Нека је $h : X \xrightarrow[\text{на}]{1-1} Y$ нека бијекција између X и Y. Тада се, аналогно претходном случају, дефинише бијекција између m и n, што према последици 4 (2) значи да је $m = n$, тј. $|X| = |Y|$.



(3) Доказ остављамо за вежбу. □

▼ Бесконачни скупови. Кантор-Бернштајнова теорема

Нису сви скупови коначни. На пример, скуп $\mathbb{N}$ није коначан: ако би за неки природан број n постојала бијекција $f : \mathbb{N} \xrightarrow[\text{на}]{1-1} n$, онда би њена рестрикција на скуп n' била 1-1 функција, $f\,|_{n'} : n' \xrightarrow{1-1} n$, супротно Дирихлеовом принципу. Скупове који нису коначни називамо **бесконачним**.

Упоређивање бесконачних скупова по „броју" елемената дефинишемо по узору на тврдње (2) и (3) теореме 31, које се односе на коначне скупове.

Дефиниција 24. *(1) Скупови A и B су* **исте кардиналности** *(имају исти број елемената), у означи $|A| = |B|$ ако постоји бијекција између A и B.*
(2) Кардиналност скупа A је мања од или једнака кардиналности скупа B, у означи $|A| \leqslant |B|$ ако постоји 1-1 функција из A у B.

Теорема 32. *За произвољне скупове A, B, C важи:*
(1) $|A| = |A|$;
(2) ако је $|A| = |B|$, онда је $|B| = |A|$;
(3) ако је $|A| = |B|$ и $|B| = |C|$, онда је $|A| = |C|$.

Доказ. (1) $\mathrm{id}_A : A \xrightarrow[\text{на}]{1-1} A$.
(2) Ако $f : A \xrightarrow[\text{на}]{1-1} B$, онда $f^{-1} : B \xrightarrow[\text{на}]{1-1} A$.
(3) Ако $f : A \xrightarrow[\text{на}]{1-1} B$ и $g : B \xrightarrow[\text{на}]{1-1} C$, онда $g \circ f : A \xrightarrow[\text{на}]{1-1} C$. □

Теорема 33. *За произвољне скупове A, B, C важи:*
(1) $|A| \leqslant |A|$;
(2) ако је $|A| \leqslant |B|$ *и* $|B| \leqslant |C|$, *онда је* $|A| \leqslant |C|$.

ДОКАЗ. Тврђење (1) директно следи из претходне теореме. Тврђење (2) је последица чињенице да из $f : A \overset{1-1}{\to} B$ и $g : B \overset{1-1}{\to} C$ следи $g \circ f : A \overset{1-1}{\to} C$. □

Теорема 34. [***Кантор-Бернштајнова теорема***] *Нека су A и B било који скупови. Ако је $|A| \leqslant |B|$ и $|B| \leqslant |A|$, онда је $|A| = |B|$.*

Феликс Бернштајн (1878–1956), немачки математичар

Најпре доказујемо једну корисну лему.

Лема 9. [***Тарски***] *Нека је A било који скуп и $F : \mathcal{P}(A) \to \mathcal{P}(A)$ функција која задовољава следећи услов:*

$(*)$ $$(\forall X, Y \in \mathcal{P}(A))\, X \subseteq Y \Rightarrow F(X) \subseteq F(Y).$$

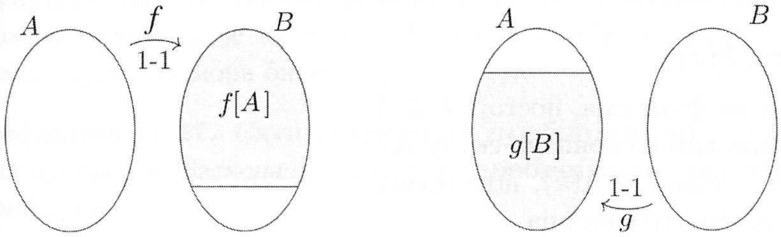
Тада постоји $E \subseteq A$ такав да је $F(E) = E$.

ДОКАЗ. Нека је $\mathcal{E} = \{X \mid X \subseteq A \wedge X \subseteq F(X)\}$ и $E = \bigcup \mathcal{E}$. Доказаћемо да је E *фиксна тачка* функције F, тј. $F(E) = E$. Приметимо најпре да важи:

$$E = \bigcup_{X \in \mathcal{E}} X \subseteq \bigcup_{X \in \mathcal{E}} F(X) \overset{(!)}{\subseteq} F(\bigcup_{X \in \mathcal{E}} X) = F(E).$$

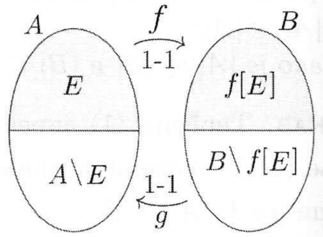
Инклузија означена знаком узвика важи јер за свако $X \in \mathcal{E}$, $X \subseteq \bigcup X$ и $F(X) \subseteq F(\bigcup_{X \in \mathcal{E}} X)$, према $(*)$. Из услова $(*)$ добијамо и да је $F(E) \subseteq F(F(E))$, одакле следи да $F(E) \in \mathcal{E}$, па је $F(E) \subseteq \bigcup \mathcal{E} = E$. Дакле, $F(E) = E$. □

ДОКАЗ. [**Кантор-Бернштајнова теорема**] Нека $f : A \overset{1-1}{\to} B$ и $g : B \overset{1-1}{\to} A$. Очигледно је да се помоћу функције f може дефинисати бијекција између скупова A и $f[A]$, а помоћу функције g бијекција међу скуповима B и $g[B]$. Међутим, могуће је да скупови $f[A]$ и $g[B]$ буду прави подскупови, редом од B и A.



Наравно, слично запажање важи и за подскупове од A, одн. B: ако је $X \subseteq A$, онда f одређује једну бијекцију између X и $f[X]$, а ако је $Y \subseteq B$, онда g одређује бијекцију између Y и $g[Y]$. Кључно питање је да ли постоји подскуп $E \subseteq A$ такав да g одређује бијекцију између $B \setminus f[E]$ и $A \setminus E$, тј. да важи

$$g[B \setminus f[E]] = A \setminus E, \text{ одн. } E = A \setminus g[B \setminus f[E]].$$



Другим речима, треба испитати да ли постоји фиксна тачка функције $F : \mathcal{P}(A) \to \mathcal{P}(A)$, $F(X) = A \setminus g[B \setminus f[X]]$, $X \in \mathcal{P}(A)$. Према претходној леми, довољно је проверити да ли важи услов $(*)$. За било које $X_1, X_2 \subseteq A$ важи:

$$\begin{aligned} X_1 \subseteq X_2 &\Rightarrow f[X_1] \subseteq f[X_2] \\ &\Rightarrow B \setminus f[X_1] \supseteq B \setminus f[X_2] \\ &\Rightarrow g[B \setminus f[X_1]] \supseteq g[B \setminus f[X_2]] \\ &\Rightarrow A \setminus g[B \setminus f[X_1]] \subseteq A \setminus g[B \setminus f[X_2]] \\ &\Leftrightarrow F(X_1) \subseteq F(X_2). \end{aligned}$$

Према претходној леми, постоји скуп E такав да је $F(E) = E$, тј. $g[B \setminus f[E]] = A \setminus E$. Приметимо да за свако $x \in A \setminus E$, постоји јединствени (јер је g 1-1 функција) елемент из B чија је g-слика једнака x; тај јединствени елемент из B означићемо са $g^{-1}(x)$. Сада није тешко дефинисати жељену бијекцију. Нека је $h : A \to B$ функција дата са:

$$h(x) = \begin{cases} f(x), & x \in E, \\ g^{-1}(x), & x \in A \setminus E \end{cases}$$

Доказ да је h бијекција остављамо за вежбу. □

Упоређивање бесконачних скупова по кардиналности (по броју елемената) има смисла јер се испоставља да постоје разне врсте бесконачности и да од сваког бесконачног скупа постоји неки „бесконачнији", тј. веће кардиналности.

Дефиниција 25. *Кардиналност скупа A је мања од кардиналности скупа B, у ознаци $|A| < |B|$, ако је $|A| \leqslant |B|$ и $|A| \neq |B|$.*

Теорема 35. *За сваки скуп A, $|A| < |\mathcal{P}(A)|$.*

Доказ. Није тешко уочити да је $|A| \leqslant |\mathcal{P}(A)|$. Заиста, функција $f : A \to \mathcal{P}(A)$, $f(x) = \{x\}$, $x \in A$, јесте 1-1 функција.

Остаје још да покажемо да не постоји бијекција између A и $\mathcal{P}(A)$. Претпоставимо супротно, да $h : A \xrightarrow[\text{на}]{1-1} \mathcal{P}(A)$. Дефинишимо скуп

$$K = \{x \in A \mid x \notin h(x)\}.$$

Очигледно $K \in \mathcal{P}(A)$, па пошто је h на функција, постоји $k \in A$ такав да је $h(k) = K$. Да ли k припада или не припада скупу K?
1. *могућност*: $k \in K$. Из $h(k) = K$ следи $k \in h(k)$, што према дефиницији скупа K, значи да $k \notin K$. Контрадикција.
2. *могућност*: $k \notin K$. Из $h(k) = K$ следи $k \notin h(k)$, што према дефиницији скупа K, значи да $k \in K$. Контрадикција.

Из добијених контрадикција закључујемо да не постоји бијекција између A и $\mathcal{P}(A)$. □

Доказ последње теореме је стар преко сто година. На основу доказане неједнакости можемо конструисати бесконачан, строго

растући по кардиналности, низ бесконачних скупова:

$$|\mathbb{N}| < |\mathcal{P}(\mathbb{N})| < |\mathcal{P}(\mathcal{P}(\mathbb{N}))| < \cdots < |\underbrace{\mathcal{P}(\cdots\mathcal{P}(\mathcal{P}}_{n}(\mathbb{N}))\cdots)| < \cdots$$

▾ Пребројиви и непребројиви скупови

Дефиниција 26. *Скуп X је* ***пребројив*** *ако је $|X| = |\mathbb{N}|$.*

Да је X пребројив означава се и $|X| = \aleph_0$.

Алеф $\aleph$ је прво слово семитских алфабета.

Теорема 36. *Сваки подскуп пребројивог скупа је коначан или пребројив.*

Доказ. Доказаћемо да је сваки бесконачан подскуп од $\mathbb{N}$ пребројив. Из тога једноставно следи опште тврђење.

Нека је A бесконачан подскуп од $\mathbb{N}$. Будући да је $|A| \leqslant |\mathbb{N}|$ (функција $f : A \to \mathbb{N}$, $f(a) = a$, $a \in A$, јесте 1-1 функција), према Кантор-Бернштајновој теореми треба још показати да је $|\mathbb{N}| \leqslant |A|$.

Дефинишимо најпре један низ подскупова од A. Применом теореме рекурзије дефинишемо $E : \mathbb{N} \to \mathcal{P}(A)$:

$$\begin{cases} E_0 = \emptyset, \\ E_{n+1} = E_n \cup \{\min(A \setminus E_n)\}. \end{cases}$$

Једноставно се доказују следеће чињенице:

- за свако $n \in \mathbb{N}$, E_n је коначан подскуп од A, па је и $A \setminus E_n \neq \emptyset$;[143]
- E је строго растући (у односу на инклузију) низ, што значи да за све $m, n \in \mathbb{N}$, из $m < n$ следи $E_m \subset E_n$;
- за свако $n \in \mathbb{N}$ и свако $m > n$, $\min(A \setminus E_n) \in E_m$.

[143] Ако би било $A \setminus E_n = \emptyset$, имали бисмо $A \subseteq E_n$, одакле би следило да је A коначан скуп (видети задатак 2 на стр. 134).

Нека је $h : \mathbb{N} \to A$, $h(n) = \min(A \setminus E_n)$. Докажимо да је h 1-1 функција. Претпоставимо да је $n_1 \neq n_2$. Без губљења општости можемо узети да је $n_1 < n_2$. Из $h(n_1) = \min(A \setminus E_{n_1}) \in E_{n_2}$, закључујемо да мора бити $h(n_1) \neq h(n_2)$. □

Слободније говорећи, функцију h можемо посматрати као низ елемената скупа A, без понављања чланова, који је рекурзивно дефинисан:

$$h_0 = \min A$$
$$h_{n+1} = \min(A \setminus \{h_0, \dots, h_n\})$$

Дефиниција 27. *Скуп је* ***највише пребројив*** *ако је коначан или пребројив. Бесконачан скуп је* ***непребројив*** *ако није највише пребројив.*

Из претходне теореме следи да је сваки подскуп пребројивог скупа највише пребројив.

Теорема 37. *Скуп A је највише пребројив акко је $|A| \leqslant |\mathbb{N}|$.*

Теорема 38. *Ако постоји функција из $\mathbb{N}$ на скуп A, $f : \mathbb{N} \xrightarrow{\text{na}} A$, онда је A највише пребројив.*

Доказ. Нека $f : \mathbb{N} \overset{\text{на}}{\to} A$. Тада је за свако $a \in A$, скуп

$$f^{-1}[\{a\}] = \{n \in \mathbb{N} \mid f(n) = a\}$$

непразан подскуп од $\mathbb{N}$, па самим тим има најмањи елемент. Нека је $g : A \to \mathbb{N}$ функција дефинисана са: $g(a) = \min f^{-1}[\{a\}]$, $a \in A$. Функција g је 1-1 функција, јер уколико је $a_1 \neq a_2$, онда мора бити $f^{-1}[\{a_1\}] \cap f^{-1}[\{a_2\}] = \emptyset$, па је $g(a_1) \neq g(a_2)$. Тиме је доказано $|A| \leqslant |\mathbb{N}|$, што значи да је A највише пребројив. □

▼ Задаци и додаци

1. Нека је n било који природан број.
(а) Сваки подскуп a од n је коначан и важи $|a| \leqslant n$.
(б) За сваки $a \subset n$ не постоји бијекција између n и a.
(в) За сваку функцију f из n у n важи: $f : n \overset{1-1}{\to} n$ акко $f : n \overset{\text{на}}{\to} n$.
2. Нека је X коначан скуп.
(а) Сваки подскуп A од X је коначан и важи $|A| \leqslant |X|$.
(б) За сваки $A \subset X$ не постоји бијекција између X и A.
(в) За сваку функцију f из X у X важи: $f : X \overset{1-1}{\to} X$ акко $f : X \overset{\text{на}}{\to} X$.
3. Нека су X и Y произвољни коначни скупови. Доказати:
(а) [Принцип збира] Ако је $X \cap Y = \emptyset$, онда је $|X \cup Y| = |X| + |Y|$;
(б) [Принцип производа] $|X \times Y| = |X| \cdot |Y|$.
4. Доказати:
(а) Ако су X и Y коначни скупови, онда је

$$|X \cup Y| + |X \cap Y| = |X| + |Y|.$$

(б) Унија два коначна скупа је коначан скуп.
(в) Декартов производ два коначна скупа је коначан скуп.
5. (а) Колико има функција из m у n?
(б) Колико има 1-1 функција из m у n?
(в) Колико има на функција из m у n?
6. Доказати:
(а) Скуп $\mathbb{N} \times \mathbb{N}$ је пребројив. Уопште, Декартов производ два пребројива скупа је пребројив.
(б) За свако $n \geqslant 3$, скуп $\mathbb{N}^n$ је пребројив.
(в) Пребројива унија пребројивих скупова је пребројив скуп.
(г) Скуп коначних низова пребројивог скупа је пребројив.
(д) Скуп коначних подскупова пребројивог скупа је пребројив.
7. Нека је $2^{\mathbb{N}}$ скуп свих бинарних низова (тј. функција из $\mathbb{N}$ у $\{0,1\}$). Доказати да је скуп $2^{\mathbb{N}}$ непребројив.
8. Ако је $|A| = |B|$ и $|C| = |D|$, доказати:
(а) $|A \times C| = |B \times D|$ (б) $|A^C| = |B^D|$

Y^X је ознака скупа свих функција из X у Y.

9. Доказати да за произвољне скупове A, B, C важи:
(а) $|A^{B \cup C}| = |A^B \times A^C|$, уколико је $B \cap C = \emptyset$
(б) $|(A \times B)^C| = |A^C \times B^C|$
(в) $|(A^B)^C| = |A^{B \times C}|$

4.2. Аксиома избора

Увод. Претходни одељак је завршен теоремом 38 (страна 133): ако постоји функција из $\mathbb{N}$ **на** скуп A, $f : \mathbb{N} \stackrel{\text{na}}{\to} A$, онда постоји и 1-1 функција из A у $\mathbb{N}$, тј. $|A| \leqslant |\mathbb{N}|$.

Да ли важи општије тврђење: ако постоји функција из X **на** скуп A, $f : X \stackrel{\text{na}}{\to} A$, онда је $|A| \leqslant |X|$ (постоји и 1-1 функција из A у X)? Кључну улогу у доказу поменуте теореме 38 има добро уређење скупа $\mathbb{N}$. То запажање директно доводи до следећег уопштења.

Дефиниција 28. *Уређење $\preceq$ неког скупа X је* ***добро*** *ако сваки непразан подскуп од X има најмањи елемент у односу на $\preceq$.*

Подсећамо да је свако добро уређење такође линеарно. Заиста, за свака два елемента x и y доброг уређења, подскуп $\{x, y\}$ има најмањи елемент, па мора бити $x \leqslant y$ или $y \leqslant x$. Наравно, обратно није тачно у општем случају: линеарно уређење не мора бити добро.

Лема 10. *Ако на скупу X постоји неко добро уређење и $f : X \stackrel{\text{na}}{\to} A$, онда је $|A| \leq |X|$.*

Доказ. Нека је $\preceq$ добро уређење скупа X и $f : X \stackrel{\text{na}}{\to} A$. Тада је за свако $a \in A$, скуп

$$f^{-1}[\{a\}] = \{x \in X \mid f(x) = a\}$$

непразан подскуп од X, па самим тим има најмањи елемент у односу на $\preceq$. Нека је $g : A \to X$ функција дефинисана са:

$$g(a) = \min_{\preceq} f^{-1}[\{a\}],\ a \in A.$$

$\min_{\preceq}$ означава најмањи елемент у односу на $\preceq$.

Функција g је 1-1, јер из $a_1 \neq a_2$ следи $f^{-1}[\{a_1\}] \cap f^{-1}[\{a_2\}] = \emptyset$, па мора бити $g(a_1) \neq g(a_2)$. Дакле, $|A| \leqslant |X|$. □

Основна улога доброг уређења у претходном доказу јесте да обезбеди функцију која из непразних подскупова од X издваја по један елемент; управо таква је функција $\min_{\preceq} : \mathcal{P}(X) \setminus \{\emptyset\} \to X$, јер $\min_{\preceq}(Y) \in Y$, за свако непразно $Y \subseteq X$. Очигледно је да се може доказати и следеће тврђење.

Лема 11. *Ако постоји функција $F : \mathcal{P}(X) \setminus \{\emptyset\} \to X$, таква да $F(Y) \in Y$, за свако непразно $Y \subseteq X$, и $f : X \stackrel{\text{na}}{\to} A$, онда је $|A| \leq |X|$.*

Одговор на полазно питање зависи од одговора на следеће питање: да ли за сваки скуп X постоји функција $F : \mathcal{P}(X) \setminus \{\emptyset\} \to X$, таква да је $F(Y) \in Y$, за непразно $Y \subseteq X$? Испоставља се да **ZF** не може да „одговори" на ово тврђење ни потврдно ни одрично.

План
- Аксиома избора (AC)
- Цорнова лема (ZL); Цермелова лема (WO); (AC) $\Leftrightarrow$ (ZL) $\Leftrightarrow$ (WO)
- Теорема о ултрафилтеру; бесконачна верзија Ремзијеве теореме

ZFC је теорија **ZF** проширена Аксиомом избора, краће (AC).

ZFC = ZF + AC
AC је скраћеница назива на енглеском језику, **A**xiom of **C**hoice.

> Аксиома избора
> Ако је $\mathcal{A}$ скуп чији су сви елементи непразни, онда постоји (тзв. *изборна*) функција $f : \mathcal{A} \to \cup\mathcal{A}$ таква да за све $X \in \mathcal{A}$, $f(X) \in X$.

Једноставна последица Аксиоме избора јесте следеће тврђење:

(AC*) за сваки скуп A постоји функција $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, таква да за све X, $\emptyset \neq X \subseteq A$, важи $f(X) \in X$.

Није тешко уочити да из (AC*) следи Аксиома избора. Заиста, нека је $\mathcal{A}$ произвољан скуп чији су сви елементи неки непразни скупови. Нека је $A = \cup\mathcal{A}$. Тада, према (AC*) постоји функција $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, таква да за све X, $\emptyset \neq X \subseteq A$, важи $f(X) \in X$. Будући да је $\mathcal{A} \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$, директно следи да је $f \restriction \mathcal{A}$ изборна функција за $\mathcal{A}$.

Подсећамо на задатак 4, на страни 91, да је $\mathcal{A} \subseteq \mathcal{P}(\cup\mathcal{A})$, за било које $\mathcal{A}$.

Аксиома избора има доста еквивалентних формулација. Једна од најпознатијих је Цорнова лема.

Дефиниција 29. *Нека је $(P, \leq)$ уређење (тј. $\leq$ је релација поретка на скупу P).*

(1) Скуп $L \subseteq P$ је ланац ако су свака два елемента из L упоредива у односу на $\leq$, тј. за све $x, y \in L$ важи $x \leq y$ или $y \leq x$.

(2) Скуп $X \subseteq P$ је одозго ограничен ако постоји елемент $a \in P$ такав да за све $x \in X$ важи $x \leq a$.

(3) Елемент $a \in P$ је максималан ако <u>не постоји</u> елемент $x \in P$ такав да је $a \leq x$ и $a \neq x$.

Пример 51. Пре него што формулишемо Цорнову лему, размотрићемо постојање максималног елемента у коначним и пребројивим уређењима. Нека је $\leqslant$ уређење скупа X.

Ако је X коначан скуп, јасно је да постоји максималан елемент. До тог елемента долазимо следећим поступком:

бирамо произвољни елемент $a_0 \in X$; постоје две могућности:

постоји $a_1 > a_0$, иначе је a_0 максималан;

постоји $a_2 > a_1$, иначе је a_1 максималан;

итд.

Пошто је X коначан, поступак се мора завршити и напослетку налазимо максималан елемент.

Ако је X пребројив, претходни поступак се не мора завршити; добијамо ланац који увек можемо изнова продужити. Међутим,

ако сваки ланац има горње ограничење, доћи ћемо до максималног елемента.

Поређајмо најпре све елементе скупа X у низ (без понављања): нека $x : \mathbb{N} \overset{1-1}{\underset{\text{na}}{\rightarrow}} X$, и у складу са тим пишемо $X = \{x_0, x_1, x_2, \ldots\}$. Дефинишимо један нови низ елемената из X:

- $a_0 = x_0$,
- $a_{n+1} = x_{k_n}$, где је k_n најмањи индекс такав да је $x_{k_n} > a_n$.

Очигледно, $a_0 < a_1 < a_2 < a_3 < \cdots$ је један ланац елемената из X. Ако сваки ланац има горње ограничење, онда постоји елемент $y \in X$ такав да је $a_n < y$, за свако $n \in \mathbb{N}$. Међутим, како је $y = x_m$, за неко $m \in \mathbb{N}$, закључујемо да се мора завршити поступак који нас је довео да посматраног ланца, а самим тим долазимо до максималног елемента.

Теорема 39. [***Цорнова лема*** (ZL)] *Нека је $(P, \leq)$ уређење. Ако је сваки ланац у P одозго ограничен, онда у $(P, \leq)$ постоји максималан елемент.*

Макс Цорн (1906–1993), немачки математичар

Доказ. Претпоставимо да је сваки ланац у $(P, \leq)$ одозго ограничен, али да ово уређење нема максималан елемент.

Према овим претпоставкама, за сваки ланац L у $(P, \leq)$, постоји елемент $u \in P$ који је горње оганичење за L, тј. $x \leq u$, за свако $x \in L$, и елемент v такав да је $u < v$, јер $(P, \leq)$ нема максималан елемент; елемент v је тзв. *строго* (наравно, горње) ограничење ланца L. Нека је $\mathcal{O}_L$ скуп свих строгих ограничења ланца L; јасно, $\mathcal{O}_L \neq \varnothing$ за сваки ланац L. Према аксиоми избора, постоји изборна функција f скупа $\{\mathcal{O}_L \mid L \text{ је ланац у } (P, \leq)\}$. Дакле, $f(L) \in \mathcal{O}_L$, тј. $f(L)$ је једно строго ограничење ланца L.

Ако је L ланац у $(P, \leq)$ и $x \in L$, нека је $(-, x)_L \overset{\text{def}}{=} \{y \in L \mid y < x\}$; скуп $(-, x)_L$ називамо иницијални сегмент ланца L. Главну улогу у доказу имају добро уређени (у односу на $\leq$) ланци, који су извесном смислу 'генерисани' функцијом f. Прецизније, скуп $A \subseteq P$ називамо *f-низ*[151] ако важе следећа два услова:

- $\leq$ је добро уређење на скупу A;
- за сваки $x \in A$, $f\left((-, x)_A\right) = x$.

Кључно запажење јесте: унија f-низова је такође f-низ. Одатле следи, ако је $\mathcal{D}$ скуп свих f-низова у P, онда је $D = \cup\mathcal{D}$ такође f-низ. Нека је $d = f(D)$, строго ограничење скупа D. Међутим, скуп $D \cup \{d\}$ је такође f-низ, одакле следи да $D \cup \{d\} \in \mathcal{D}$, тј. $D \cup \{d\} \subseteq \cup\mathcal{D} = D$, одакле следи $d \in D$, што је немогуће.

Преостаје само да докажемо да је унија f-низова такође f-низ. Доказ те чињенице излажемо у наредне три леме.

Лема 1. *Ако су A и B два f-низа и $A \neq B$, онда је један од њих иницијални сегмент другог.*

[151] Назив овакве врсте скупова није важан нити је устаљен. Уопштено, f-низови генерализују идеју 'обичног' низа генерисаног функцијом f. Полазимо најпре од $\varnothing$, који јесте ланац, и бирамо произвољан елемент скупа P, $f(\varnothing) = a_0$. Сваки једночлани скуп јесте ланац; нека је $f(\{a_0\}) = a_1$. Будући да је $a_0 < a_1$, $\{a_0, a_1\}$ је ланац; нека је $f(\{a_0, a_1\}) = a_2$ (одакле следи $a_0 < a_1 < a_2$) итд. Сваки f-низ A јесте ланац (свако добро уређење је линеарно) и може се проширити до новог f-низа: ако је $f(A) = a$, онда је $A \cup \{a\}$ такође f-низ.

Доказ леме 1. Из $A \neq B$ следи да је $A \setminus B \neq \emptyset$ или $B \setminus A \neq \emptyset$. Без губљења општости можемо претпоставити да је $A \setminus B \neq \emptyset$ и нека је x најмањи елемент скупа $A \setminus B$; $x = \min(A \setminus B)$. Тада је очигледно $(-,x)_A \subseteq B$. Доказаћемо да је заправо $(-,x)_A = B$.

Претпоставимо да је $B \setminus (-,x)_A \neq \emptyset$ и $y = \min(B \setminus (-,x)_A)$. Тада је $(-,y)_B \subseteq (-,x)_A$. Нека је даље $z = \min(A \setminus (-,y)_B)$; јасно $(-,z)_A \subseteq (-,y)_B$ и $z \leq x$. Дакле, $(-,z)_A \subseteq (-,y)_B \subseteq (-,x)_A$.

(I) Ако је $z = x$, онда је $(-,z)_A = (-,y)_B = (-,x)_A$.

(II) Ако је $z < x$, пошто $z \in A$, онда $z \in (-,x)_A \subseteq B$, одакле следи $y \leq z$, па мора бити и $(-,z)_A \supseteq (-,y)_B$; дакле $(-,z)_A = (-,y)_B$.

Из претпоставке да су A и B f-низови, следи да је

$$y = f((-,y)_B) = f((-,z)_A) = z \in (-,x)_A,$$

што је немогуће према избору елемента y, у случају (II). И у случају (I) долазимо до контрадикције јер $x \notin (-,x)_A$. Дакле, $(-,x)_A = B$. Другим речима, из $A \setminus B \neq \emptyset$ следи да је B почетни сегмент скупа A. Наравно, из $B \setminus A \neq \emptyset$ следи да је A почетни сегмент скупа B. Овим је лема 1 доказана.

Лема 2. *Ако је A f-низ и $x \in A$, онда из $y < x$ следи да $y \in A$ или y не припада ниједном f-низу у P.*

Доказ леме 2. Нека је A f-низ, $x \in A$, $y < x$ тако да $y \notin A$, али $y \in C$, за неки f-низ C. Из леме 1 следи да је A иницијални сегмент од C (јасно је да C не може бити иницијални сегмент од A). Међутим, тада из $y < x$ и $x \in A$ следи да $y \in A$. Контрадикција. Овим је доказана лема 2.

Лема 3. *Унија f-низова је такође f-низ.*

Доказ леме 3. Нека је $\mathcal{C}$ неки скуп f-низова.

Докажимо прво да је $\bigcup \mathcal{C}$ добро уређен. Нека је $\emptyset \neq D \subseteq \bigcup \mathcal{C}$, и $C \in \mathcal{C}$, такав да је $\emptyset \neq D \cap C$. Како је $D \cap C$ непразан подскуп од C који је добро уређен релацијом $\leq$, постоји $x = \min(D \cap C)$. Претпоставимо да D садржи и елемент y такав да је $y < x$; очигледно $y \notin C$. Према леми 2, следи да y не припада ниједном f-низу, што значи да $y \notin \bigcup \mathcal{C}$. Самим тим, $y \notin D$. Контрадикција. Дакле, D не садржи елементе мање од x, па је x најмањи елемент у D.

Докажимо и да за свако $x \in \bigcup \mathcal{C}$, важи $f((-,x)_{\bigcup \mathcal{C}}) = x$. Нека је $x \in \bigcup \mathcal{C}$ произвољан. Тада постоји $C \in \mathcal{C}$ такав да је $x \in C$. Очигледно је $(-,x)_C \subseteq (-,x)_{\bigcup \mathcal{C}}$. Нека је $y \in \bigcup \mathcal{C}$ произвољан елемент такав да је $y < x$. Из $y \in \bigcup \mathcal{C}$ следи да y припада бар једном f-низу, па према леми 2. следи да $y \in C$. Доказана је и обратна инклузија, $(-,x)_C \supseteq (-,x)_{\bigcup \mathcal{C}}$. Дакле $(-,x)_C = (-,x)_{\bigcup \mathcal{C}}$, па је $f((-,x)_{\bigcup \mathcal{C}}) = f((-,x)_C) = x$. Доказана је и лема 3. □

У уводним разматрањима је поменуто да свако добро уређење неког скупа X одређује једну функцију која из непразних подскупова од X бира по један елемент. Да ли постојање изборне

функције на скупу X имплицира постојање доброг уређења на X?

Теорема 40. [***Цермелова лема*** (WO)] *Сваки скуп се може добро уредити.*

Подсећамо, уређење је **добро**, ако сваки непразан подскуп има најмањи елемент. Постоји врло једноставна алтернативна карактеризација добрих уређења. Нека је $\preceq$ линеарно уређење скупа W. Тада је $\preceq$ добро уређење скупа W акко не постоји строго опадајући (у односу на $\preceq$) низ елемената скупа W, тј. не постоји функција $f : \mathbb{N} \to W$ таква да за све $m, n \in \mathbb{N}$, из $m < n$ следи $f_m \prec f_n$.

Цермелова лема очигледно важи за највише пребројиве (коначне и пребројиве) скупове, и то можемо показати без Аксиоме избора. Међутим, да бисмо добро уредили неки непребројив скуп, неопходно је позивање на Аксиому избора.

Доказ. Применом Цорнове леме доказујемо да постоји добро уређење на било ком скупу S.

Нека је S произвољан скуп и

$$\mathcal{W}_S = \{(A, W_A) \mid A \in \mathcal{P}(S) \text{ и } W_A \subseteq A \times A \text{ је добро уређење}\}$$

Јасно, $\mathcal{W}_S \neq \emptyset$, јер се сваки највише пребројив подскуп $A \subseteq S$ може добро уредити. Дефинишемо бинарну релацију $\preceq$ на $\mathcal{W}_S$:

$$\begin{aligned}(A, W_A) \preceq (B, W_B) \quad &\Leftrightarrow \quad (A, W_A) \text{ је почетни сегмент од } (B, W_B)\\ &\Leftrightarrow \quad 1)\ A \subseteq B,\\ &\qquad\quad 2)\ W_B \cap (A \times A) = W_A,\\ &\qquad\quad 3)\ (\forall a \in A)(\forall b \in B \setminus A)\, aW_Bb.\end{aligned}$$

Једноставно се проверава да је $\preceq$ уређење на $\mathcal{W}_S$. Нека је $\mathcal{C}$ произвољан ланац у $(\mathcal{W}_S, \preceq)$ и $D = \bigcup_{(C, W_C) \in \mathcal{C}} C$. Дефинишимо релацију W_D на скупу D: за $s, t \in D$,

$$sW_Dt \overset{\text{def}}{\Leftrightarrow} sW_Ct, \text{ за неко } (C, W_C) \in \mathcal{C} \text{ такво да } s, t \in C.$$

Очигледно је W_D коректно дефинисана релација, јер из чињенице да је $\mathcal{C}$ ланац, следи да је

$$sW_Dt \Leftrightarrow sW_Ct, \text{ за све } (C, W_C) \in \mathcal{C} \text{ такве да } s, t \in C.$$

Једноставно се проверава да је W_D уређење на D. Докажимо да је то уређење добро. Нека је $A \subseteq D$ непразан скуп. Тада постоји неко $(C, W_C) \in \mathcal{C}$ за које је $A \cap C \neq \emptyset$. Нека је a_C минималан елемент скупа $A \cap C$, у односу на W_C. Уколико је $A \cap C' \neq \emptyset$, за неки други $(C', W_{C'}) \in \mathcal{C}$, онда је једно од добрих уређења (C, W_C) и $(C', W_{C'})$ почетни сегмент другог, одакле следи да је $a_C = a_{C'}$. Одавде следи да је $(D, W_D) \in \mathcal{W}_S$ горње ограничење ланца $\mathcal{C}$. Према Цорновој леми, $\mathcal{W}_S$ има максималан елемент; нека је то (M, W_M). Доказаћемо да је $M = S$.

Ако би постојало $s \in S \setminus M$, на скупу $M' = M \cup \{s\}$ можемо дефинисати добро уређење:

$$W_{M'} = W_M \cup \{(t, s) \mid t \in M'\},$$

па бисмо имали $(M', W_{M'}) \in \mathcal{W}_S$ супротно максималности елемента (M, W_M). Дакле, $M = S$, што даље значи и да је $W_S = W_M$ добро уређење скупа S. □

Теорема 41. *Следећа тврђења су међусобно еквивалентна:*

(AC*) *За сваки скуп A постоји функција $f : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, таква да за све X, $\emptyset \neq X \subseteq A$, важи $f(X) \in X$.*

(ZL) *Нека је $(P, \leq)$ уређење. Ако је сваки ланац у P одозго ограничен, онда у $(P, \leq)$ постоји максималан елемент.*

(WO) *Сваки скуп се може добро уредити.*

Доказ. Већ је доказано (AC*) $\Rightarrow$ (ZL) и (ZL) $\Rightarrow$ (WO). Једноставно се уочава да важи и (WO) $\Rightarrow$ (AC*). Заиста, ако је $\leq$ добро уређење скупа A, онда сваки непразан подскуп има најмањи елемент, што значи да постоји функција $\min : \mathcal{P}(A) \setminus \{\emptyset\} \to A$ таква да за све X, $\emptyset \neq X \subseteq A$, $\min(X) \in X$ (и $\min(X) \leq x$, за свако $x \in X$, што није важно за овај доказ). □

▼ Теорема о ултрафилтеру

Појам филтера (и посебно, ултрафилтера) веома је значајан и налази се у основи концепта конвергенције на којима почивају бројне области савремене математике. Уопштено говорећи, филтер окупља 'велике' подскупове неког задатог скупа и често се посматра као нова врста квантификатора, о чему ће више речи бити на крају одељка.

Дефиниција 30. *Филтер на скупу S је скуп $\mathcal{B}$ подскупова од S (тј. $\mathcal{B} \subseteq \mathcal{P}(S)$) такав да:*

(B1) $\emptyset \notin \mathcal{B}$ и $S \in \mathcal{B}$ (Празан скуп није велики. Скуп S јесте велики.)

(B2) ако $A, B \in \mathcal{B}$, онда $A \cap B \in \mathcal{B}$ (Пресек два велика скупа је велики скуп.)

(B3) ако $A \in \mathcal{B}$ и $A \subseteq B$, онда $B \in \mathcal{B}$ (Надскуп великог скупа је велики скуп.)

Пример 52. Нека је S бесконачан скуп. Кажемо да је $A \subseteq S$ ко-коначан скуп, ако је његов комплемент, $S \setminus A$ коначан. Сви ко-коначни подскупови од S чине један филтер.

(B1) $S \setminus S = \emptyset$ је коначан; дакле S је ко-коначан. Наравно, како је S бесконачан, скуп $\emptyset$ није ко-коначан.

(B2) Нека су $A, B \subseteq S$ ко-коначни, тј. $S \setminus A$ и $S \setminus B$ су коначни скупови. Тада је и скуп $(S \setminus A) \cup (S \setminus B) = S \setminus (A \cap B)$ коначан, одакле следи да је $A \cap B$ ко-коначан.

(B3) Нека је $A \subseteq S$ ко-коначан, тј. $S \setminus A$ је коначан скуп. Ако је $A \subseteq B$, тада је $S \setminus B \subseteq S \setminus A$, па је и $S \setminus B$ коначан скуп, одакле следи да је B ко-коначан.

Дефиниција 31. *Нека је S произвољан бесконачан скуп. Скуп*

$$\mathcal{F}^{\infty} \stackrel{\text{def}}{=} \{A \subseteq S \mid S \setminus A \text{ је коначан скуп}\}$$

назива се кофинитан или Фрешеов филтер на S.

Морис Фреше (1878–1973), француски математичар

Ако све филтере на неком скупу уредимо инклузијом, није тешко доказати да ће $\subseteq$-ланци филтера бити одозго ограничено. Према Цорновој леми, закључујемо да постоје и максимални филтери – тзв. ултрафилтери. У наредној леми ћемо доказати постојање ултрафилтера који проширује Фрешеов филтер.

Дефиниција 32. *Ултрафилтер на S јесте филтер на S који је максималан у смислу инклузије.*

Пре него што докажемо најављену теорему, изводимо једно важно својство ултрафилтера.

Лема 12. *Нека је $\mathcal{U}$ ултрафилтер на S. Тада за сваки скуп $D \subseteq S$, или $D \in \mathcal{U}$ или $S \setminus D \in \mathcal{U}$ (али не оба).*

Доказ. Нека је $\mathcal{U}$ ултрафилтер на S и $D \subseteq S$ такав да $D \notin \mathcal{U}$ и $S \setminus D \notin \mathcal{U}$. Нека је

$$\mathcal{B}_D = \{X \subseteq S \mid (\exists U \in \mathcal{U})\, U \cap D \subseteq X\}.$$

Доказаћемо да је $\mathcal{B}_D$ филтер на S.
(B1) Из $S \in \mathcal{U}$ и $S \cap D \subseteq S$, следи да $S \in \mathcal{B}_D$. Ако би било $\emptyset \in \mathcal{B}_D$, постојао би $U \in \mathcal{U}$, такав да је $U \cap D \subseteq \emptyset$, тј. $U \subseteq S \setminus D$, одакле би следило $S \setminus D \in \mathcal{U}$, супротно претпоставци. Дакле, $\emptyset \notin \mathcal{B}_D$.
(B2) Ако $A, B \in \mathcal{B}_D$, онда постоје $U_1, U_2 \in \mathcal{U}$ такви да је $U_1 \cap D \subseteq A$ и $U_2 \cap D \subseteq B$. Тада је $(U_1 \cap U_2) \cap D \subseteq A \cap B$, па како $U_1 \cap U_2 \in \mathcal{U}$, следи да $A \cap B \in \mathcal{B}_D$.
(B3) Нека је $A \in \mathcal{B}_D$ и $A \subseteq B$. Тада постоји $U \in \mathcal{U}$ такав да је $U \cap D \subseteq A$, а самим тим је $U \cap D \subseteq B$, па $B \in \mathcal{B}_D$.

Очигледно је $\mathcal{U} \subseteq \mathcal{B}_D$. Штавише, $\mathcal{U} \subset \mathcal{B}_D$, јер $D \notin \mathcal{U}$, али $D \in \mathcal{B}_D$. То је контрадикција са максималношћу филтера $\mathcal{U}$, у односу на инклузију. □

Теорема 42. [*Теорема о ултрафилтеру*] *Сваки филтер на S је садржан у неком ултрафилтеру.*

Доказ. Нека је

$$\Phi = \{\mathcal{B} \mid \mathcal{B} \text{ је филтер на } S \text{ и } \mathcal{F} \subseteq \mathcal{B}\},$$

скуп свих филтера који садрже $\mathcal{F}$. Очигледно, $\mathcal{F} \in \Phi$ и $\subseteq$ је уређење на Φ.

Нека је Λ ланац у $(\Phi, \subseteq)$. Дакле, за филтере $\mathcal{B}_1, \mathcal{B}_2 \in \Lambda$, важи $\mathcal{B}_1 \subseteq \mathcal{B}_2$ или $\mathcal{B}_2 \subseteq \mathcal{B}_1$.

Доказаћемо да је $\mathcal{L} = \bigcup \Lambda$ филтер на S.
(B1) $S \in \mathcal{B}$, за свако $\mathcal{B} \in \Lambda$; дакле, $S \in \bigcup \Lambda = \mathcal{L}$. За свако $\mathcal{B} \in \Lambda$, $\emptyset \notin \mathcal{B}$; дакле, $\emptyset \notin \bigcup \Lambda = \mathcal{L}$.
(B2) Ако $A, B \in \bigcup \Lambda$, онда постоје $\mathcal{B}_1, \mathcal{B}_2 \in \Lambda$ такви да $A \in \mathcal{B}_1$ и $B \in \mathcal{B}_2$. Како је $\mathcal{B}_1 \subseteq \mathcal{B}_2$ или $\mathcal{B}_2 \subseteq \mathcal{B}_1$, закључујемо да $A, B \in \mathcal{B}_1$ или $A, B \in \mathcal{B}_2$, и самим тим, $A \cap B$ припада једном од филтера $\mathcal{B}_1$ или $\mathcal{B}_2$, одакле следи да $A \cap B \in \bigcup \Lambda = \mathcal{L}$.

(В3) Нека је $A \in \bigcup \Lambda$ и $A \subseteq B$. Постоји $\mathcal{B} \in \Lambda$ такав да $A \in \mathcal{B}$, па мора бити и $B \in \mathcal{B}$, одакле следи да $B \in \bigcup \Lambda = \mathcal{L}$.

Јасно, за свако $\mathcal{B} \in \Lambda$, $\mathcal{B} \subseteq \mathcal{L}$, одакле следи да је филтер $\mathcal{L}$ горње ограничење ланца Λ.

Према Цорновој леми, $(\Phi, \subseteq)$ има максималан елемент. Максималан елемент је тражени ултрафилтер над S, који проширује филтер $\mathcal{F}$. □

Ултрафилтер $\mathcal{U}$ на S можемо посматрати и као квантификатор. У том случају, подскуп $A \subseteq S$ посматрамо као унарну релацију на S и:

- уместо $s \in A$ користимо запис $A(s)$,
- уместо $A \in \mathcal{U}$ пишемо $(\mathcal{U}s)A(s)$; нови запис читамо *за $\mathcal{U}$-скоро све s из S важи $A(s)$*.

Посебно је важна чињеница да се квантификатор $\mathcal{U}$ лепо слаже са логичким везницима.

Лема 13. *Нека је $\mathcal{U}$ ултрафилтер на S и $A, B \subseteq S$.*
(1) $(\forall s)\, A(s) \Rightarrow (\mathcal{U}s)\, A(s)$
(2) $\neg(\mathcal{U}s)\, A(s) \;\Leftrightarrow\; (\mathcal{U}s) \neg A(s)$
(3) $(\mathcal{U}s)\, (A(s) \wedge B(s)) \Leftrightarrow (\mathcal{U}s)\, A(s) \wedge (\mathcal{U}s)\, B(s)$
(4) $(\mathcal{U}s)\, (A(s) \vee B(s)) \Leftrightarrow (\mathcal{U}s)\, A(s) \vee (\mathcal{U}s)\, B(s)$

Упутство. Доказ наведених особина квантификатора произлазе из следећих особина ултрафилтера:
(1) $S \in \mathcal{U}$
(2) $A \in \mathcal{U} \;\Leftrightarrow\; S \setminus A \notin \mathcal{U}$ (и наравно, $A \notin \mathcal{U} \;\Leftrightarrow\; S \setminus A \in \mathcal{U}$)
(3) $A \cap B \in \mathcal{U} \;\Leftrightarrow\; A \in \mathcal{U}$ и $B \in \mathcal{U}$
(4) $A \cup B \in \mathcal{U} \;\Leftrightarrow\; A \in \mathcal{U}$ или $B \in \mathcal{U}$

Последица 5. *Нека је $\mathcal{U}$ ултрафилтер на S и $A_1, \ldots, A_n$ коначно много подскупова од S. Ако је $(\mathcal{U}s)\, (A_1(s) \vee \cdots \vee A_n(s))$, онда је $(\mathcal{U}s)\, A_k(s)$, за тачно једно $k \in \{1, \ldots, n\}$.*

Примену ултрафилтера илуструјемо у доказу једног веома значајног комбинаторног резултата који има широку примену. Реч је о теореми која у извесном смислу представља уопштење бесконачне верзије Дирихлеовог принципа: *ако је сваки елемент неког бесконачног скупа обојен једном од две боје, тада постоји једнобојан бесконачан подскуп тог скупа*, што је једноставна последица чињенице да је унија два коначна скупа такође коначан скуп.

Теорема 43. [*Ремзијева теорема*][154] *Претпоставимо да је сваки пар природних бројева обојен једном од две боје: белом или црном. Тада постоји бесконачан подскуп X од $\mathbb{N}$ такав да су сви парови елемената од X обојени истом бојом.*

Доказ. Сваком пару природних бројева, који чине различити природни бројеви m и n, придружујемо јединствен уређен пар (m, n), такав да је $m < n$. Нека $B(m, n)$ значи да је одговарајући пар обојен белом бојом, а $C(m, n)$ да је пар обојен црном бојом.

[154] Франк Ремзи (1903–1930), енглески математичар
Ако је $\mathbb{N}^{[2]}$ скуп свих двочланих подскупова од $\mathbb{N}$, бојење парова природних бројева у две боје јесте функција $f : \mathbb{N}^{[2]} \to \{0, 1\}$, при чему 0 и 1 представљају две боје. У формулацији теореме је коришћено слободније изражавање да би се јасније истакла сама суштина тврђења.

Теорему ћемо доказати ако конструишемо низ $a_1 < a_2 < \dots$ природних бројева такав да је $B(a_i, a_j)$, за све $i < j$ или је $C(a_i, a_j)$, за све $i < j$.

Јасно је да важи $(\forall m)(\forall n > m)(B(m,n) \vee C(m,n))$. Нека је $\mathcal{U}$ ултрафилтер који проширује Фрешеов филтер.

За свако фиксирано $m \in \mathbb{N}$,

$$\{n > m \mid B(m,n)\} \cup \{n > m \mid C(m,n)\} = \mathbb{N} \setminus \{0, 1, \dots, m\} \in \mathcal{U},$$

одакле следи да $\{n > m \mid B(m,n)\}$ или $\{n > m \mid C(m,n)\}$ припада $\mathcal{U}$. Дакле, $(\forall m)((\mathcal{U}n)\, B(m,n) \vee (\mathcal{U}n)\, C(m,n))$. Даље,

$$\{m \mid (\mathcal{U}n)\, B(m,n)\} \cup \{m \mid (\mathcal{U}n)\, C(m,n)\} = \mathbb{N} \in \mathcal{U},$$

одакле следи да $\{m \mid (\mathcal{U}n)\, B(m,n)\}$ или $\{m \mid (\mathcal{U}n)\, C(m,n)\}$ припада $\mathcal{U}$. Добијамо: $(\mathcal{U}m)\,(\mathcal{U}n)\, B(m,n) \vee (\mathcal{U}m)\,(\mathcal{U}n)\, C(m,n)$.

Претпоставимо прво да је $(\mathcal{U}m)\,(\mathcal{U}n)\, B(m,n)$, тј. *$\mathcal{U}$-скоро сви елементи m имају својство да за $\mathcal{U}$-скоро све елементе n важи* $B(m,n)$. Тада једноставно конструишемо бесконачан расући низ чији ће сви парови чланова бити бели:

– прво бирамо a_1 такав да је $(\mathcal{U}n)\, B(a_1, n)$;

– затим бирамо $a_2 > a_1$ такав да је $B(a_1, a_2)$ и $(\mathcal{U}n)\, B(a_2, n)$

> такав постоји, јер из $(\mathcal{U}n)\, B(a_1, n) \wedge (\mathcal{U}m)\,(\mathcal{U}n)\, B(m,n)$, уз преименовање везаних променљивих, изводимо закључак $(\mathcal{U}n)\,(B(a_1, n) \wedge (\mathcal{U}m)\, B(n,m))$

– затим бирамо $a_3 > a_2$ такав да је $B(a_1, a_3)$, $B(a_2, a_3)$ и $(\mathcal{U}n)\, B(a_3, n)$

> из $(\mathcal{U}n)\, B(a_1, n) \wedge (\mathcal{U}n)\, B(a_2, n) \wedge (\mathcal{U}m)\,(\mathcal{U}n)\, B(m,n)$ следи $(\mathcal{U}n)\,(B(a_1, n) \wedge B(a_2, n) \wedge (\mathcal{U}m)\, B(n,m))$, па постоји a_3 са жељеним особинама.

итд.

Настављајући наведени поступак, добијамо тражени низ.

Аналогно поступамо у случају да је $(\mathcal{U}m)\,(\mathcal{U}n)\, C(m,n)$. □

Није тешко уочити да Ремзијеву теорему можемо доказати и у општијем случају, када k-точлане подскупове од $\mathbb{N}$ бојимо у коначно боја.

Теорема 44. [***Бесконачна верзија Ремзијеве теореме***] *Нека је $k, r \geqslant 1$. Ако је сваки k-точлани подскуп од $\mathbb{N}$ обојен једном од r боја, онда постоји бесконачан подскуп X од $\mathbb{N}$ такав да су k-точлани подскупови од X обојени истом бојом.*

▼ Задаци и додаци

1. Ако $g : X \overset{\text{на}}{\to} Y$, доказати да је $|Y| \leq |X|$.

2. Нека је $R \subseteq A \times B$ релација између A и B, чији је домен A, тј. $(\forall a \in A)(\exists b \in B)\, R(a,b)$. Доказати да постоји подскуп $F \subseteq R$ који је функција из A у B.

3. Доказати да се сваки највише пребројив скуп може добро уредити.

4. Доказати да је лексикографско уређење скупа $\mathbb{N}\times\mathbb{N}$

$$(m_1, n_1) \leqslant_{\text{lex}} (m_2, n_2) \;\Leftrightarrow\; m_1 < m_2 \vee (m_1 = m_2 \wedge n_1 \leqslant n_2),$$

добро уређење.

Додатак

Нека је $\leqslant$ добро уређење скупа W. Почетни сегмент је сваки скуп облика $(-,x) = \{y \in W \mid y < x\}$, $x \in X$, називамо почетним (иницијалним) сегментима.

---

5. Нека је $\leqslant$ добро уређење скупа W и $A \subseteq W$. Ако за свако $x \in W$ важи:

$$(*) \qquad x \in A \Rightarrow (-,x) \subseteq A,$$

доказати да је $A = W$ или је A почетни сегмент. Додатно, ако је $A \neq W$, онда је $A = (-,a)$, где је $a = \min(W \setminus A)$.

6. [156] Нека је $\leqslant$ добро уређење скупа W. Ако је $A \subseteq W$ такав да за свако $x \in W$ важи

$$(\star) \qquad (-,x) \subseteq A \Rightarrow x \in A,$$

онда је $A = W$.

[156] Тврђење задатка је познато и као *Принцип трансфинитне индукције*.

7. Нека је $(W,\preceq)$ добро уређење и $f: W \to W$ монотона функција, тј. функција таква да за све $x_1, x_2 \in W$

$$x_1 \prec x_2 \Rightarrow f(x_1) \prec f(x_2).$$

Тада за свако $x \in W$ важи $x \preceq f(x)$.

Упутство. Применити тврђење из претходног задатка.

8. *Ординал* је скуп α који задовољава следећа два својства:

- релација $\in$ је добро уређење скупа α;
- ако $x \in \alpha$, онда је $x \subset \alpha$.

Доказати:

(а) Почетни сегмент ординала је ординал.

(б) Сваки елемент ординала је ординал.

(в) Ако је α ординал, онда је и $\alpha \cup \{\alpha\}$ такође ординал.

9. Ако су X и Y произвољни скупови, применом Цорнове леме доказати да је $|X| \leqslant |Y|$ или $|Y| \leqslant |X|$.

Упутство. Нека је $\mathcal{B} = \{f \mid f: U \xrightarrow[\text{na}]{1-1} V$, за неке $U \subseteq X, V \subseteq Y\}$ и $\preceq$ релација на $\mathcal{B}$ дефинисана са:

$$f \preceq g \overset{\text{def}}{\Leftrightarrow} \operatorname{dom}(f) \subseteq \operatorname{dom}(g) \wedge (\forall x \in \operatorname{dom}(f))\,(f(x) = g(x)).$$

Доказати најпре да је $\preceq$ уређење на $\mathcal{B}$ у коме је сваки ланац одозго ограничен. Према Цорновој леми, у $\mathcal{B}$ постоји $\preceq$-максималан елемент $F: U \xrightarrow[\text{na}]{1-1} V$, за неке $U \subseteq X, V \subseteq Y$; доказати да мора бити $U = X$ или $V = Y$.

10. Применом Цорнове леме, доказати да за сваки бесконачан скуп X:

(а) $|X| = |(X \times \{0\}) \cup (X \times \{1\}|$; (б) $|X| = |X \times X|$.

11. Ако је A бесконачан скуп, доказати да је $|\mathbb{N}| \leqslant |A|$.

Напомена. Скуп A је бесконачан, па за свако $n \in \mathbb{N}$ не постоји

$f : A \to n$, која је бијекција. Нека је $\mathcal{N}$ скуп свих коначних низова елемената из A:

$$\mathcal{N} = \{f \mid f : n \to A, n \in \mathbb{N}\}.$$

За $f : m \to A$ и $g : n \to A$, нека је

$$f \preceq g \overset{\text{def}}{\Leftrightarrow} m < n \wedge (\forall i < m)\, f(i) = g(i);$$

$\preceq$ је заправо релација 'почетни сегмент'. Приметити да $\mathcal{N}$ не садржи максималан елемент; што значи да постоји ланац $\mathcal{L}$ који није одозго ограничен. Користећи тај ланац дефинисати функцију $n \to x(n)$, где је $x \in \mathcal{L}$ било који елемент ланца чија је дужина већа од n. Треба доказати да је ова функција коректно дефинисана.

12. Ако је A бесконачан скуп и B пребројив скуп, доказати да је $|A \cup B| = |A|$.

Напомена. Ако је A бесконачан, онда је $|\mathbb{N}| \leqslant |A|$, па постоји 1-1 функција $a : \mathbb{N} \to A$, тј. бесконачан низ елемената скупа A без понављања. Скупови $B \cup \{a_0, a_1, \ldots\}$ и $\{a_0, a_1, \ldots\}$ су исте кардиналности.

13. Ако је A непребројив скуп и B пребројив скуп, доказати да је $|A \setminus B| = |A|$.

14. Нека је S непразан скуп и $s \in S$. Доказати да је скуп свих подскупова од S који садрже s, тј. $\mathcal{F}_s = \{X \in \mathcal{P}(S) \mid s \in X\}$ филтер на S.

15. Нека су X и Y непразни скупови и $f : X \overset{\text{na}}{\to} Y$. Тада, ако је $\mathcal{U}$ ултрафилтер на X, доказати да је $\mathcal{V} = \{f[U] \mid U \in \mathcal{U}\}$ ултрафилтер на Y.

16. Нека је S непразан скуп и нека $\mathcal{B} \subseteq \mathcal{P}(S)$ има својство *коначог пресека*: пресек коначно много елемената из $\mathcal{B}$ је непразан; тј. за коначно много скупова $B_1, \ldots, B_n \in \mathcal{B}$, $n \geqslant 1$, $B_1 \cap \cdots \cap B_n \neq \emptyset$.

(а) Доказати да је скуп

$$\mathcal{F} = \{X \in \mathcal{P}(S) \mid B_1 \cap \cdots \cap B_n \subseteq X, \text{ за неке } B_1, \ldots, B_n \in \mathcal{B}, n \geqslant 1\}$$

филтер на S.

(б) Доказати да постоји ултрафилтер $\mathcal{U}$ на S који садржи $\mathcal{B}$.

Упутство. Доказ је веома сличан доказу леме 12, на страни 141.

4.3. Структуре првог реда

УВОД. Појам математичке структуре заузима централно место у савременој математици.[157] Уопштено говорећи, математичку структуру чини неки скуп, такозвани *домен*, *носач* или *универзум* структуре, заједно са релацијама и операцијама дефинисаним над доменом. Издвајамо један пример типичне структуре, коју чине:

- скуп $\mathbb{N}^+ = \{1, 2, 3, 4, \ldots\}$,
- бинарне операције: сабирање $(+)$, множење $(\cdot)$, степеновање $(\uparrow)$, при чему уместо $m \uparrow n$ краће пишемо m^n, и
- константа 1.

Ову структуру краће означавамо као уређену петорку, наводећи све оно што је чини: $(\mathbb{N}^+, +, \cdot, \uparrow, 1)$. Средином шездесетих година 20. века, Алфред Тарски је проучавао законитости које важе у овој структури, полазећи од основних идентитета које је назвао *средњошколским идентитетима*:

$$
(HSI) \begin{cases}
\forall x \forall y (x + y = y + x) \\
\forall x \forall y \forall z (x + (y + z) = (x + y) + z) \\
\forall x (x \cdot 1 = x) \\
\forall x \forall y (x \cdot y = y \cdot x) \\
\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z) \\
\forall x \forall y \forall z (x \cdot (y + z) = x \cdot y + x \cdot z) \\
\forall x (x^1 = x) \\
\forall x (1^x = 1) \\
\forall x \forall y \forall z (x^{y+z} = x^y \cdot x^z) \\
\forall x \forall y \forall z ((x \cdot y)^z = x^z \cdot y^z) \\
\forall x \forall y \forall z ((x^y)^z = x^{y \cdot z})
\end{cases}
$$

Наведени идентитети су тачни и у разним другим структурама *истог типа*. Једна таква структура је $(\{0,1\}, +, \cdot, \uparrow, 1)$, са доменом $\{0,1\}$ над којим су дате три бинарне операције (дефинисане наредним таблицама) и константа 1:

$+$	0	1
0	0	1
1	1	1

$\cdot$	0	1
0	0	0
1	0	1

$\uparrow$	0	1
0	1	0
1	1	1

Није тешко уочити да операције $+$ и $\cdot$ заправо представљају редом дисјункцију и конјункцију над $\{0,1\}$, а да $x \uparrow y$, тј. x^y одговара исказној формули $y \Rightarrow x$. Једноставно је проверити да у структури $(\{0,1\}, +, \cdot, \uparrow, 1)$ важе све HSI законитости. Све структуре одговарајућег типа, које задовољавају HSI законитости називају се HSI алгебрама.

ПЛАН

- Рационални бројеви
- Структуре и њихов вокабулар
- Теорије; Семантичка и синтаксна последица

---

[157] Иако се идеја структуре, у извесном смислу, среће и у радовима Лајбница, верује се да је Шредер 1895. године први пут дефинисао појам апстрактне структуре.

Готфрид Вилхелм Лајбниц (1646–1716), немачки математичар и филозоф

Ернс Шредер (1841–1902), немачки математичар

HSI – High School Identities

Подсећамо на следеће парове еквивалентних исказних формула:

$x \vee y \equiv y \vee x$
$x \vee (y \vee z) \equiv (x \vee y) \vee z$
$x \wedge 1 \equiv x$
$x \wedge y \equiv y \wedge x$
$x \wedge (y \wedge z) \equiv (x \wedge y) \wedge z$
$x \wedge (y \vee z) \equiv (x \wedge y) \vee (x \wedge z)$
$1 \Rightarrow x \equiv x$
$x \Rightarrow 1 \equiv 1$
$y \vee z \Rightarrow x \equiv (y \Rightarrow x) \wedge (z \Rightarrow x)$
$z \Rightarrow x \wedge y \equiv (z \Rightarrow x) \wedge (z \Rightarrow y)$
$z \Rightarrow (y \Rightarrow x) \equiv z \wedge y \Rightarrow x$

▼ Рационални бројеви

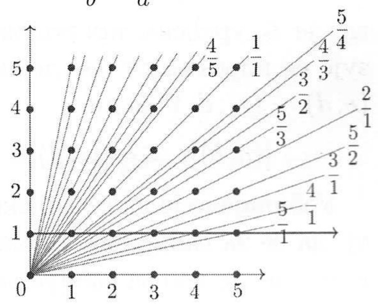
Најважније примере структура чине оне над скуповима бројева. У овом одељку укратак описујемо конструкцију ненегативних рационалних бројева. Основне идеје конструкције су свакако познате и овом приликом их само строже излажемо.

На скупу $\mathbb{N} \times \mathbb{N}^+$ дефинишемо бинарну релацију $\sim$:

$$(a,b) \sim (c,d) \;\Leftrightarrow\; a \cdot d = b \cdot c, \quad \text{за } (a,b),(c,d) \in \mathbb{N} \times \mathbb{N}^+$$

У конструкцији коју описујемо, уређени пар $(a,b) \in \mathbb{N} \times \mathbb{N}^+$ представља разломак $\frac{a}{b}$. Релација $\sim$ је заправо једнакост међу разломцима:

$$\frac{a}{b} = \frac{c}{d} \;\Leftrightarrow\; ad = bc.$$



Лема 14. *Релација $\sim$ је релација еквиваленције на $\mathbb{N} \times \mathbb{N}^+$.*

Доказ. (Р) Из $a \cdot b = b \cdot a$ следи $(a,b) \sim (a,b)$.

(С) Ако је $(a,b) \sim (c,d)$, онда је $a \cdot d = b \cdot c$, одн. $c \cdot b = d \cdot a$, па је $(c,d) \sim (a,b)$.

(Т) Нека је $(a,b) \sim (c,d)$ и $(c,d) \sim (e,f)$. Тада је $a \cdot d = b \cdot c$ и $c \cdot f = d \cdot e$. Ако је $c = 0$, онда је и $a = e = 0$ (јер је $b \neq 0$ и $d \neq 0$), па је $a \cdot f = b \cdot e$, тј. $(a,b) \sim (e,f)$. Претпоставимо да је $c \neq 0$. Тада је

$$(*) \qquad (a \cdot d) \cdot (c \cdot f) = (b \cdot c) \cdot (d \cdot e).$$

Применом комутативности и асоцијативности, трансформишемо изразе са леве и десне стране једнакости $(*)$:

$$(a \cdot d) \cdot (c \cdot f) = \cdots = (a \cdot f) \cdot (c \cdot d) \text{ и } (b \cdot c) \cdot (d \cdot e) = \cdots = (b \cdot e) \cdot (c \cdot d).$$

Из једнакости $(*)$ и последње две једнакости добијамо

$$(a \cdot f) \cdot (c \cdot d) = (b \cdot e) \cdot (c \cdot d).$$

Најзад, применом закона скраћивања (видети задатак 10 на страни 125), јер је $c \cdot d \neq 0$: $a \cdot f = b \cdot e$. Дакле, $(a,b) \sim (e,f)$. □

Количнички скуп $\mathbb{N} \times \mathbb{N}^+ / \sim$ називамо скупом ненегативних рационалних бројева и означавамо $\mathbb{Q}_{\geqslant 0}$.

Сабирање и множење на скупу $\mathbb{Q}_{\geqslant 0}$ дефинишемо користећи својства дата у следећој леми. Да бисмо поједноставили запис, изостављамо ознаку множења природних бројева и подразумевамо приоритет множења над сабирањем.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

Лема 15. *Ако је $(a,b) \sim (a_1,b_1)$ и $(c,d) \sim (c_1,d_1)$, онда је:*
(1) $(ad+bc, bd) \sim (a_1d_1 + b_1c_1, b_1d_1)$
(2) $(ac, bd) \sim (a_1c_1, b_1d_1)$

Доказ. Доказ остављамо за вежбу. Истичемо само реформулацију тврђења које треба доказати: из претпоставки $ab_1 = ba_1$ и $cd_1 = dc_1$, треба извести:
(1) $(ad+bc) \cdot (b_1d_1) = (bd) \cdot (a_1d_1 + b_1c_1)$;
(2) $(ac) \cdot (b_1d_1) = (bd) \cdot (a_1c_1)$. □

Сабирање и множење, $+_{\mathbb{Q}}, \cdot_{\mathbb{Q}} : \mathbb{Q}_{\geqslant 0} \times \mathbb{Q}_{\geqslant 0} \to \mathbb{Q}_{\geqslant 0}$ дефинишемо једнакостима:

$$[(a,b)]_\sim +_{\mathbb{Q}} [(c,d)]_\sim \overset{\text{def}}{=} [(ad+bc, bd)]_\sim, \quad [(a,b)]_\sim \cdot_{\mathbb{Q}} [(c,d)]_\sim \overset{\text{def}}{=} [(ac, bd)]_\sim.$$

Претходна лема заправо показује да су наведене дефиниција операција коректне. Наиме, операције су дефинисане у односу на изабране представнике класа еквиваленције. Лема показује да представнике можемо произвољно изабрати: увек добијамо исти резултат, које год представнике да изаберемо. Ако је $(a,b) \sim (a_1,b_1)$ и $(c,d) \sim (c_1,d_1)$, тј. $[(a,b)]_\sim = [(a_1,b_1)]_\sim$ и $[(c,d)]_\sim = [(c_1,d_1)]_\sim$, онда је:

$$[(ad+bc,bd)]_\sim = [(a_1d_1+b_1c_1,b_1d_1)]_\sim \text{ и } [(ac,bd)]_\sim = [(a_1c_1,b_1d_1)]_\sim$$

Бинарну релацију $\leqslant_\mathbb{Q}$ уводимо на следећи начин:

$$[(a,b)]_\sim \leqslant_\mathbb{Q} [(c,d)]_\sim \overset{\text{def}}{\Leftrightarrow} ad \leqslant bc,$$

$\frac{a}{b} \leqslant_\mathbb{Q} \frac{c}{d} \Leftrightarrow ad \leqslant bc$

где је $\leqslant$ уређење природних бројева. Слично претходном, доказује се коректност ове дефиниције[164], тј. да из $(a,b) \sim (a_1,b_1)$ и $(c,d) \sim (c_1,d_1)$ следи:

$$[(a,b)]_\sim \leqslant_\mathbb{Q} [(c,d)]_\sim \text{ акко } [(a_1,b_1)]_\sim \leqslant_\mathbb{Q} [(c_1,d_1)]_\sim.$$

[164] Из претпоставки $ab_1 = ba_1$, $cd_1 = dc_1$ и $ad \leqslant bc$ треба извести $a_1d_1 \leqslant b_1c_1$.

Уобичајено је да се индекс $\mathbb{Q}$ изоставља у ознакама $+_\mathbb{Q}$, $\cdot_\mathbb{Q}$, $\leqslant_\mathbb{Q}$, тј. да се за сабирање, множење и уређење целих бројева користе исте ознаке као за сабирање, множење и уређење природних бројева, што је давно усвојен обичај у случајевима када се *увођењем нових бројева, операција и релација са њима, поштују операције и релације старих бројева, тј. када је сачуван рад са старим бројевима.*[165] Наведеном конструкцијом изграђена је важна бројевна структура $(\mathbb{Q}_{\geqslant 0}, \leqslant, +, \cdot, 0, 1)$.

[165] Ово начело проширивања скупова бројева познато је и као Ханкелов принцип перманенције. Природан број n можемо идентификовати са $[n,1]_\sim$. Једноставно се показује да су при овакво идентификацији, рестрикције уведених операција на $\mathbb{Q}_{\geqslant 0}$ истоветне одговарајућим операцијама на скупу природних бројева.
Херман Ханкел (1839–1873), немачки математичар

Лема 16. *За произвољне* $x, y, z \in \mathbb{Q}_{\geqslant 0}$:

$$x+(y+z) = (x+y)+z \qquad x\cdot(y\cdot z) = (x\cdot y)\cdot z$$
$$x+y = y+x \qquad x\cdot y = y\cdot x$$
$$x+0 = x \qquad x\cdot 1 = x,\ x\cdot 0 = 0$$
$$x \neq 0 \Rightarrow (\exists u \in \mathbb{Q}_{\geqslant 0})\, x\cdot u = 1$$
$$x\cdot(y+z) = x\cdot y + x\cdot z$$
$$x \leqslant x$$
$$x \leqslant y \wedge y \leqslant x \Rightarrow x = y$$
$$x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z$$
$$x \leqslant y \vee y \leqslant x$$
$$x \leqslant y \Rightarrow x+z \leqslant y+z \qquad x \leqslant y \Rightarrow x\cdot z \leqslant y\cdot z$$

Ако $\mathbb{Q}_{>0}$ означава скуп $\mathbb{Q}_{\geqslant 0} \setminus \{0\}$, није тешко уочити да сабирање и множење представљају и операције скупа $\mathbb{Q}_{>0}$. Ослањајући се на особине из претходне леме, једноставно се доказује да за свако $x \in \mathbb{Q}_{>0}$ постоји јединствено $u \in \mathbb{Q}_{>0}$ такво да је $x \cdot u = 1$. На основу те особине уводимо унарну операцију $^{-1} : \mathbb{Q}_{>0} \to \mathbb{Q}_{>0}$, тзв. *реципрочну вредност*. На сличан начин се уводе и разне друге познате операције скупа ненегативних рационалних бројева. На пример, на основу чињенице да за све $a, b \in \mathbb{Q}_{\geqslant 0}$ постоји тачно једно $c \in \mathbb{Q}_{\geqslant 0}$ тако да $a + c = b \vee b + c = a$, уводимо важну бинарну операцију $(a,b) \mapsto c = |a-b|$.

Збир и производ бројева различитих од нуле, такође су различити од нуле

Реципрочна вредност није операција скупа $\mathbb{Q}_{\geqslant 0}$

▼ Структуре и њихов вокабулар

Уопште, операцијско-релацијску структуру чини скуп заједно са неким својим операцијама, релацијама и елементима (константама).

Читав овај одељак повезује и допуњује скоро све теме које му претходе.

Дефиниција 33. *Нека је S произвољан непразан скуп и $n \geqslant 1$.*

(1) Свака функција из S^n у S, назива се n-арна операција скупа S. Посебно, функције из S у S називамо унарним операцијама; функције из $S \times S$ у S називамо бинарним операцијама.

(2) Сваки подскуп од S^n, назива се n-арна релација скупа S. Посебно, подскупове од S називамо унарним релацијама; подскупове од $S \times S$ називамо бинарним релацијама.

$S^n = \underbrace{S \times \cdots \times S}_{n \text{ пута}}$ је скуп свих уређених n-торки елемената из S.

Ако је $R \subseteq S^n$ и $a_1, \ldots, a_n \in S$, уместо $(a_1, \ldots, a_n) \in R$ пишемо $R(a_1, \ldots, a_n)$ и читамо: „елементи $a_1, \ldots, a_n$ су у релацији R". Сваку n-арну релацију можемо посматрати као функцију из S^n у двочлани скуп $\{0, 1\}$ иснитосних вредности, и самим тим исказе „$R(a_1, \ldots, a_n)$ је тачно" и „$R(a_1, \ldots, a_n)$ је нетачно" записати редом као једнакости $R(a_1, \ldots, a_n) = 1$ и $R(a_1, \ldots, a_n) = 0$.

Структуре задајемо тако што наведемо, у облику низа, све оно што је чини. Структуре често означавамо масним словима $\mathbf{A}, \mathbf{B}, \mathbf{C}, \ldots$, по потреби са индексима, при чему углавном користимо слова којима су означени домени (носачи) тих структура, $A, B, C, \ldots$, са одговарајућим индексима.

ПРИМЕР:
Стандардну структуру природних бројева чини скуп природних бројева $\mathbb{N}$, заједно са релацијом уређења $\leqslant$, унарном операцијом следбеник $' : \mathbb{N} \to \mathbb{N}$, бинарним операцијама сабирања и множења $+, \cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, и константом 0. Искористићемо структуру $\mathbf{N} = (\mathbb{N}, \leqslant, ', +, \cdot, 0)$ да илуструјемо наредне појмове.

Вокабулар структуре
Симболи којима означавамо релације, операције и константе неке структуре називамо *вокабуларом* те структуре.

Вокабулар структуре $\mathbf{N}$ чине симболи: $\leqslant$, $'$, $+$, $\cdot$, 0

Вокабулар заједно са логичким симболима чине алфабет тзв. *језика првог реда* који користимо за описивање структуре:

ЛОГИЧКИ СИМБОЛИ
промењљиве:
$x, y, z, x_1, y_1, z_1, \ldots$

знак једнакости: $=$
логичке константе: $\perp$, $\top$
логички везници: (унарни) $\neg$,
(бинарни) $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$
квантификатори: $\forall$, $\exists$
помоћни знаци: (,)

ВОКАБУЛАР СТРУКТУРЕ
симболи константи;
симболи операција, при чему је за сваки симбол одређена његова дужина;
симболи релација, при чему је за сваки симбол одређена његова дужина.

Логички симболи су непроменљиви део језика првог реда, док симболе вокабулара одређује тип структуре коју посматрамо.

Изрази

Изразе градимо индуктивно, на уобичајен начин, користећи променљиве, симболе константи, симболе операција и помоћне знаке. Другим речима, користимо правила: $I \to c \mid v \mid F(I, \cdots, I)$, где је c симбол константе, v променљива, и F знак операције (наравно, примењен на одговарајући број једноставнијих израза).

Примери израза над вокабуларом структуре $\mathbf{N}$: 0, $0'$, $0' \cdot (0')'$, $(x+0)'$, $x+y$, $0' \cdot (x+0')$, $x \cdot x + y \cdot y$, итд. Приликом записивања израза користимо уобичајене договоре о брисању заграда, о приоритету међу операцијама и сл.

Ако је t неки израз, са $V(t)$ означићемо скуп оних променљивих које учествују у грађењу израза t. Наравно, за сваки израз t, скуп $V(t)$ је коначан:

- $V(v) = \{v\}$, за променљиву v; $V(c) = \varnothing$, за симбол константе c;
- $V(F(t_1, \ldots, t_n)) = V(t_1) \cup \cdots \cup V(t_n)$, за симбол операције F дужине n и изразе $t_1, \ldots, t_n$.

Атомске формуле

Логичке константе сматрамо атомским формулама, а остале *атомске формуле* добијамо повезивањем два израза знаком једнакости или повезивањем одговарајућег броја израза симболом релације: $A \to \top \mid \bot \mid I = I \mid R(I, \ldots, I)$, где је R симбол релације.

Примери атомских формула над вокабуларом структуре $\mathbf{N}$ су $0 = 0''$, $0 \leqslant 0$, $x \cdot 0 \leqslant x + 0$, $x + y = y + x$ итд.

Формуле

Формуле дефинишемо индуктивно. Атомске формуле су формуле; сложеније формуле добијамо применом везника на једноставније формуле и постављањем квантификатора са променљивом испред формуле: $F \to A \mid \neg F \mid (F * F) \mid \forall v\, F \mid \exists v\, F$, при чему је v променљива, а $* \in \{\vee, \wedge, \Rightarrow, \Leftrightarrow\}$.

Примери формула над вокабуларом структуре $\mathbf{N}$: $0 = x$, $0 = 0 \wedge \neg 0' \leqslant 0$, $0' \leqslant x \Rightarrow x \leqslant (x \cdot x)$, $\neg \exists x (x + 0') = 0$, $\forall x \forall y (x + y = y + x)$ итд.

Слободна и везана појављивања променљивих

Појављивање променљиве у формули може бити *слободно* или *везано.* Свако појављивање променљиве које није под дејством квантификатора назива се слободним, а она појављивања која јесу под дејством квантификатора називају се везаним.

Све променљиве које имају слободна појављивања у некој формули називају се **слободне променљиве** те формуле. Скуп свих слободних променљивих формуле α означавамо $\mathrm{Fr}(\alpha)$ и прецизно дефинишемо индукцијом по сложености формуле:

- $\mathrm{Fr}(\bot) = \mathrm{Fr}(\top) = \varnothing$;
- $\mathrm{Fr}(t_1 = t_2) = V(t_1) \cup V(t_2)$;

- $\mathrm{Fr}(R(t_1,\ldots,t_n)) = V(t_1)\cup\cdots\cup V(t_n)$;
- $\mathrm{Fr}(\neg\alpha) = \mathrm{Fr}(\alpha)$;
- $\mathrm{Fr}(\alpha * \beta) = \mathrm{Fr}(\alpha)\cup\mathrm{Fr}(\beta)$, $* \in \{\vee,\wedge,\Rightarrow,\Leftrightarrow\}$;
- $\mathrm{Fr}(\forall x\alpha) = \mathrm{Fr}(\exists x\alpha) = \mathrm{Fr}(\alpha)\setminus\{x\}$.

За сваку формулу α, скуп $\mathrm{Fr}(\alpha)$ је коначан.

Вредност израза (функције)

Изразима, над вокабуларом неке структуре $\mathbf{S}$, дефинишу се нове функције, заправо операције над S. Ако је $V(t)\subseteq\{x_1,\ldots,x_n\}$, онда израз t означавамо $t(x_1,\ldots,x_n)$ када желимо да истакнемо да су све променљиве које учествују у грађењу израза t неке од променљивих $x_1,\ldots,x_n$. Додељујући променљивама $x_1,\ldots,x_n$ редом неке вредности $a_1,\ldots,a_n$ из S, добијамо јединствену вредност $t(a_1,\ldots,a_n)\in S$:

$$S^n \ni (a_1,\ldots,a_n)\mapsto t(a_1,\ldots,a_n)\in S;$$

на овај начин је дефинисана једна функција из S^n у S (заправо n-арна операција скупа S).

Над вокабуларом структуре $\mathbf{N}$, наводимо неколико вредности функције која је дефинисана изразом $t(x_1,x_2,x_3) = x_1'\cdot(x_2+0')$:

- $t(2,1,4) = 2'\cdot(1+0') = 6$,
- $t(3,3,3) = 3'\cdot(3+0') = 16$,
- $t_5(7,13,31) = 7'\cdot(13+0') = 112$ итд.

Истинитосна вредност формуле

Приликом одређивања истинитосне вредности сложенијих формула користимо таблице исказних везника и следећа правила за квантификаторе:

- ако је $\alpha(x_1,\ldots,x_n)$ формула облика $\forall x\theta(x,x_1,\ldots,x_n)$, онда је за $a_1,\ldots,a_n\in S$,
$$\alpha(a_1,\ldots,a_n) = \min_{a\in S}\theta(a,a_1,\ldots,a_n);$$
- ако је $\alpha(x_1,\ldots,x_n)$ формула облика $\exists x\theta(x,x_1,\ldots,x_n)$, онда је за $a_1,\ldots,a_n\in S$,
$$\alpha(a_1,\ldots,a_n) = \max_{a\in S}\theta(a,a_1,\ldots,a_n).$$

Примери релација дефинисаних изразима над вокабуларом структуре $\mathbf{N}$:

- $\alpha_1(x,y)$ је $x'\leqslant y\Rightarrow x\leqslant y'$; нпр. $\alpha_1(0,0)$, $\alpha_1(0,1)$, $\alpha_1(1,0)$, $\alpha_1(0,2)$, $\alpha_1(2,0)$ су тачни искази;
- $\alpha_2(x,y)$ је формула $\exists z\,(x+z=y)$; нпр. $\alpha_2(3,0)$ је нетачно, $\alpha_2(0,3)$ је тачно, итд.
- $\alpha_3(x)$ је формула $\forall y\,(x\cdot y = x)$; нпр. $\alpha_3(0)$ је тачно, $\alpha_3(1)$ је нетачно, итд.

Ако је $\mathrm{Fr}(\alpha)\subseteq\{x_1,\ldots,x_n\}$, онда формулу α означавамо и са $\alpha(x_1,\ldots,x_n)$ када желимо да истакнемо чињеницу да су све слободне променљиве формуле α неке од променљивих $x_1,\ldots,x_n$. Додељујући променљивама $x_1,\ldots,x_n$ редом вредности $a_1,\ldots,a_n$ из M, добијамо јединствену *истинитосну* вредност $\alpha(a_1,\ldots,a_n)$:

$$S^n\ni(a_1,\ldots,a_n)\mapsto\alpha(a_1,\ldots,a_n)\in\{0,1\};$$

на овај начин је дефинисана једна функција из S^n у $\{0,1\}$, тј. једна n-арна релација скупа S.

Тачност реченице

Формула σ је **реченица** ако нема слободних променљивих, тј. ако је $\mathrm{Fr}(\alpha) = \emptyset$. На (не)истинитост реченице у некој структури не утичу вредности променљивих. Да је реченица σ тачна у некој структури $\mathbf{S}$, записујемо $\mathbf{S} \models \sigma$ и кажемо да је структура $\mathbf{S}$ *модел* реченице σ. Ако реченица σ није тачна у $\mathbf{S}$ пишемо $\mathbf{S} \not\models \sigma$ и кажемо да је $\mathbf{S}$ *контрамодел* реченице σ. Приметимо да ако $\mathbf{S} \not\models \sigma$, онда $\mathbf{S} \models \neg\sigma$.

Пример 53.
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \forall x \forall y \forall z (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \forall x \forall y (x + y = 0 \Rightarrow x = 0 \wedge y = 0)$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \forall x \forall y (x \cdot y = 0 \Rightarrow x = 0 \vee y = 0)$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \neg \forall x \forall y (x \leqslant y' \Rightarrow x' \leqslant y)$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \forall x (\neg x = 0 \Rightarrow \exists y (x = y'))$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \exists y \forall x (x \cdot y = x)$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \neg \exists x (x \cdot x = 0'')$
$(\mathbb{N}, \leqslant, ', +, \cdot, 0) \models \exists x (x \cdot x = 0'''')$
итд.

Најједноставнија класификација операцијско-релацијских структура врши се према вокабулару, тј. према броју и дужини релација и операција, као и броју константи које учествују у њиховој дефиницији. За структуре које имају исти вокабулар кажемо да су истог типа. Међу структурама истог типа издвајамо оне које задовољавају неке изабране особине, тј. задовољавају одређене *теорије*.

Дефиниција 34. *Теорија неког вокабулара јесте било који скуп реченица тог вокабулара.*

Пример 54. Издвајамо један, посебно важан пример теорије – **теорију уређених група**. Вокабулар уређених група чине следећи симболи: симбол бинарне релације, симбол бинарне операције, симбол унарне операције и симбол константе; у општем случају, често се користе следећи симболи: $\leq$, $*$, $^{-1}$, e. Теорију уређених група Γ_{OG} чине следеће реченице:
(R) $\forall x \ (x \leq x)$
(AS) $\forall x \forall y \ (x \leq y \wedge y \leq x \Rightarrow x = y)$
(T) $\forall x \forall y \forall y \ (x \leq y \wedge y \leq z \Rightarrow x \leq z)$
(A) $\forall x \forall y \forall z \ (x * (y * z) = (x * y) * z)$
(N) $\forall x \ (x * e = x)$
(I) $\forall x \ (x * x^{-1} = e)$
(S) $\forall x \forall y \forall z \ (x \leq y \Rightarrow x * z \leq y * z \wedge z * x \leq z * y)$

Уређена група је свака структура $(G, \leq, *, ^{-1}, e)$ која задовољава наведене аксиоме. На пример, структура $(\mathbb{Q}_{>0}, \leqslant, \cdot, ^{-1}, 1)$ јесте пример уређене групе.

▼ Семантичка и синтаксна последица

Један од најважнијих логичких концепата јесте појам *последице*. Уводимо две врсте последице – *семантичку последицу* и *синтаксну последицу*.

Дефиниција 35. *Нека је Γ нека теорија (скуп реченица). Реченица α је* ***семантичка последица*** *теорије Γ, у ознаци $\Gamma \models \alpha$, ако за сваку структуру* **S**,

$$\text{из } \mathbf{S} \models \gamma, \text{ за свако } \gamma \in \Gamma, \text{ следи да } \mathbf{S} \models \alpha.$$

Уместо $\emptyset \models \alpha$ пишемо $\models \alpha$.

Формула α је **семантичка** последица скупа претпоставки Γ ако је α тачно у **свим структурама** у којима су тачне претпоставке из Γ.

Ако је $\models \alpha$, тј. α је тачно у свим структурама одговарајућег вокабулара, кажемо да је α **ваљана** реченица.

Посебно истичемо да знак $\models$ користимо двојако:

- као ознаку односа између структуре и реченице; $\mathbf{S} \models \alpha$ значи да је α **тачно** у структури **S**;
- као ознаку односа између скупа реченица и једне реченице; $\Gamma \models \alpha$ значи да је α **семантичка последица** скупа реченица Γ.

Пример 55. Трагање за особинама уређених група, тј. тврђењима која су тачна у свим уређеним групама представља потрагу за последицама претпоставки које се узете за аксиоме теорије уређених група. На пример, да ли у уређеним групама важи:

$$\forall x \forall y \forall z (x * z \leq y * z \Rightarrow x \leq y)?$$

Ако Γ_{OG} означава теорију уређених група, а σ горњу реченицу, питање је да ли важи $\Gamma_{\mathrm{OG}} \models \sigma$. Одговор је потврдан.

Нека је $(G, \leq, *, ^{-1}, e)$ произвољна група.

1. Изаберимо произвољне x, y, z из G, такве да је $x * z \leq y * z$.

Тада је

2. $(x * z) * z^{-1} \leq (y * z) * z^{-1}$, [сагласност $\leq$ и $*$]

3. $x * (z * z^{-1}) \leq y * (z * z^{-1})$, [из претходног према закону асоцијативности]

4. $x * e \leq y * e$, [из претходног јер је $z * z^{-1} = e$]

5. $x \leq y$, [из претходног јер је $x * e = x$ и $y * e = y$]

6. $\forall x \forall y \forall z (x * z \leq y * z \Rightarrow x \leq y)$. [јер су x, y, z произвољни елементи]

Иако током овог доказа, замишљамо да радимо са неком конкретном (произвољно изабраном) уређеном групом, није било потребе да се прецизира о којој је заиста групи реч, већ смо искључиво користили законитости које група задовољава по дефиницији, као и добро позната својства једнакости и операција (функција). Другим речима, значајне су само аксиоме теорије група, док 'семантика' није од пресудног значаја.

Претходни пример указује на концепт синтаксне последице, који је већ разматран у систему природне дедукције. Наводимо кратак резиме правила природне дедукције која смо до сада разматрали и најављујемо нова правила за језик првог реда.

- Прво смо разматрали правила природне дедукције за *исказни језик* чије су формуле грађене од исказних слова, логичке константе $\bot$ и логичких везника $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$, $\neg$.
- Затим смо разматрања проширили на *предикатски језик*, у којој су исказна слова замењена атомским формулама и додати су квантификатори $\forall$ и $\exists$; претходним правилима додата су и правила за квантификаторе.
- У наставку разматрамо формуле *језика првог реда*, које садрже богатији скуп атомских формула: релацијским симболима се повезују изрази (који могу да садрже и операцијске знаке, а не само променљиве и симболе константи, као у случају чистог предикатског језика), и додатно, као атомске формуле се појављују и једнакости; уз одговарајућа уопштења правила за квантификаторе, додајемо и правила за једнакост.

Дефиниција 36. *Ако је Γ нека теорија (скуп реченица). Реченица α је* ***синтаксна последица*** *теорије Γ, ако се секвент $\Gamma \vdash \alpha$ може добити применом правила исказне логике (страна 60) и следећих правила за квантификаторе и једнакости:*

$$(\forall x_{\mathrm{E}})\ \frac{\forall x\alpha}{\alpha[x/t]} \qquad (\exists x_{\mathrm{U}})\ \frac{\alpha[x/t]}{\exists x\alpha}$$

$$(\forall x_{\mathrm{U}})\ \frac{\begin{array}{|l} v \\ \quad\vdots \\ \quad\alpha[x/v] \end{array}}{\forall x\alpha} \qquad (\exists x_{\mathrm{E}})\ \frac{\exists x\alpha \quad \begin{array}{|l} v \quad \alpha[x/v] \\ \quad\vdots \\ \quad\gamma \end{array}}{\gamma}$$

$$(=_{\mathrm{U}})\ \frac{}{t=t} \qquad (=_{\mathrm{E}})\ \frac{\alpha[x/t] \quad t=u}{\alpha[x/u]}$$

Важно! (1) Формула $\alpha[x/t]$ означава формулу која је добија истовременом заменом свих слободних појављивања променљиве x у формули α изразом t, при чему ниједна променљива израза t не постаје везана након замене.
(2) У поддоказима правила $(\forall x_{\mathrm{U}})$ и $(\exists x_{\mathrm{E}})$, појављује се тзв. *свежа променљива* v која се у формулама ван поддоказа не појављује слободно.

Лема 17. *1.* $\vdash \forall x_1 \forall x_2 (x_1 = x_2 \Rightarrow x_2 = x_1)$

2. $\vdash \forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$

Доказ. (1) Изводимо секвент $\vdash \forall x_1 \forall x_2 (x_1 = x_2 \Rightarrow x_2 = x_1)$:

1.	x_1, x_2	Уводимо свеже променљиве да бисмо доказали $\forall x_1 \forall x_2 \cdots$;
2.	$x_1 = x_2$	додатна претпоставка;
		Нека је $\alpha(x)$ формула $x = x_1$;
3.	$x_1 = x_1$	$(=_{\mathrm{U}})$; једнакост $x_1 = x_1$ је заправо формула $\alpha[x/x_1]$;
4.	$x_2 = x_1$	$(=_{\mathrm{E}})$, 3, 2; једнакост $x_2 = x_1$ је заправо формула $\alpha[x/x_2]$;
5.	$x_1 = x_2 \Rightarrow x_2 = x_1$	$(\Rightarrow_{\mathrm{U}})$, 2-4;
6.	$\forall x_1 \forall x_2 (x_1 = x_2 \Rightarrow x_2 = x_1)$	$\forall x_{1\mathrm{U}}$, $\forall x_{2\mathrm{U}}$ 1-5

(2) Изводимо секвент $\forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$:

1.	x_1, x_2, x_3	Уводимо свеже промењиве;
2.	$x_1 = x_2 \wedge x_2 = x_3$	додатна претпоставка;
		Нека је $\alpha(x)$ формула $x_1 = x$;
3.	$x_1 = x_2$	$(\wedge^{\mathrm{L}}_{\mathrm{E}})$; једнакост $x_1 = x_2$ је $\alpha[x/x_2]$;
4.	$x_2 = x_3$	$(\wedge^{\mathrm{D}}_{\mathrm{E}})$;
5.	$x_1 = x_3$	$(=_{\mathrm{E}})$, 3, 4; једнакост $x_1 = x_3$ је $\alpha[x/x_3]$;
6.	$x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3$	$(\Rightarrow_{\mathrm{U}})$, 2-5;
7.	$\forall x_1 \forall x_2 \forall x_3 (x_1 = x_2 \wedge x_2 = x_3 \Rightarrow x_1 = x_3)$	$\forall x_{1\mathrm{U}}, \forall x_{2\mathrm{U}}, \forall x_{3\mathrm{U}}$ 1-6 □

Изведена правила могу знатно да олакшају доказивање секвената. У наредној леми дајемо неколико изведених правила која се односе на једнакости.

Лема 18.

$$\frac{t_1 = t_2}{t_2 = t_1}(=_{\mathrm{S}}) \qquad \frac{t_1 = t_2 \quad t_2 = t_3}{t_1 = t_3}(=_{\mathrm{T}}) \qquad \frac{t_1 = t_2}{t[x/t_1] = t[x/t_2]}(=_{\mathrm{sup}})$$

Доказ. Наводимо само доказ правила $(=_{\mathrm{sup}})$. Наравно, $t[x/t_1]$ је израз добијен истовременом заменом свих појављивања промењиве x у t изразом t_1.

Нека је $\alpha(y)$ формула $t[x/t_1] = t[x/y]$.

1.	$t_1 = t_2$	претпоставка;
2.	$t[x/t_1] = t[x/t_1]$	$(=_{\mathrm{U}})$; једнакост $t[x/t_1] = t[x/t_1]$ је $\alpha[y/t_1]$;
3.	$t[x/t_1] = t[x/t_2]$	$(=_{\mathrm{E}})$, 2, 1; једнакост $t[x/t_1] = t[x/t_2]$ је $\alpha[y/t_2]$. □

Пример 56. Из теорије уређених група Γ_{OG} може се извести формула $\forall x \forall y \forall z (x * z \leq y * z \Rightarrow x \leq y)$, применом правила природне дедукције. Извођење секвента

$$\Gamma_{\mathrm{OG}} \vdash \forall x \forall y \forall z (x * z \leq y * z \Rightarrow x \leq y)$$

веома је блиско доказу који је дат у примеру 55, на страни 153. Издвајамо само неколико карактеристичних корака извођења.

1.	$\forall x \forall y \forall z (x \leq y \Rightarrow x * z \leq y * z \wedge z * x \leq z * y)$	претпоставка из Γ_{OG}
	$\vdots$	
$i.$	x, y, z	уводимо свеже промењиве;
$(i+1).$	$x * z \leq y * z$	додатна претпоставка;
	$\vdots$	
$j.$	$(x * z) * z^{-1} \leq (y * z) * z^{-1}$	из 1. $\forall x_E, [x/x]; \forall y_E, [y/z];$
	$\vdots$	$\forall z_E, [z/z^{-1}]; (\Rightarrow_E); (\wedge^D_E)$
$n.$	$x \leq y$	
$(n+1).$	$x * z \leq y * z \Rightarrow x \leq y$	$(\Rightarrow_U)$, $(i+1).$-$n.$
	$\forall x \forall y \forall z (x * z \leq y * z \Rightarrow x \leq y)$	$\forall x_U, \forall y_U, \forall z_U$, $i.$-$(n+1)$.

Иако су семантичка последица ($\models$) и синтаксна последица ($\vdash$) дефинисане на сасвим различите начине, поседују низ заједничких особина. Еквивалентност ова два концепта успостављају теореме 45 и 46 (страна 156), које наводимо без доказа.

Теорема 45. [***Теорема сагласности***] *Ако је* $\Gamma \vdash \alpha$, *онда је* $\Gamma \models \alpha$.

[**Теорема сагласности**] Ако се формула α може доказати (извести) из претпоставки Γ, онда је α тачно у свим моделима скупа Γ.

Специјално, ако је α формула $\bot$, онда:

$$\text{Из } \Gamma \vdash \bot \text{ следи } \Gamma \models \bot.$$

Ако $\Gamma \vdash \bot$, кажемо да је Γ *противречан* скуп формула; $\Gamma \models \bot$ значи да Γ нема модел, тј. не постоји структура у којој су тачне све формуле из Γ. Краће речено: *Противречан скуп формула нема модел.*

Теорему сагласности можемо формулисати и у овом облику:

$$\text{Ако } \Gamma \not\models \alpha, \text{ онда } \Gamma \nvdash \alpha.$$

$\Gamma \not\models \alpha$ значи да постоји структура $\mathbf{S}$ која задовољава све реченице скупа Γ, али не задовољава α, тј. $\mathbf{S} \models \Gamma$ и $\mathbf{S} \not\models \alpha$. Претходна теорема, исказана у овом облику, често се користи да би се показало да се нека реченица *не може* доказати из датих претпоставки. На овај начин се, на пример, доказује да чувена аксиома паралелности није последица осталих аксиома еуклидске геометрије.

Пример 57. Докажимо да се закон комутативности, тј. формула $\forall x \forall y (x * y = y * x)$ не може извести из аксиома теорије група T_{G}:
(A) $\forall x \forall y \forall z\ (x * (y * z) = (x * y) * z)$
(N) $\forall x\ (x * e = x)$
(I) $\forall x\ (x * x^{-1} = e)$.

Да бисмо доказали да $T_{\mathrm{G}} \nvdash \forall x \forall y (x * y = y * x)$, довољно је доказати да $T_{\mathrm{G}} \not\models \forall x \forall y (x * y = y * x)$, за шта је довољно да конструишемо групу чија бинарна операција није комутативна. Једна од њих је група $(S_3, \circ, ^{-1}, \sigma_1)$, где је S_3 скуп свих пермутација (бијекција) скупа $\{1, 2, 3\}$ чију су елементи[172]:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Да група није комутативна показују једнакости:

$$\tau_3 \circ \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_2, \ \tau_2 \circ \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_3.$$

[172] Структура $(S_3, \circ, ^{-1}, \sigma_1)$ је група, према тврђењу задатка 12 на страни 161.

Тачан је обрат теореме сагласности.

Теорема 46. [***Теорема потпуности***][173] *Ако је* $\Gamma \models \alpha$, *онда је* $\Gamma \vdash \alpha$.

[173] Теорему потпуности први је доказао Гедел.

Одељак завршавамо примерима који илуструју значај развоја дедуктивних система у различитим областима.

Пример 58. Претпоставимо да вокабулар садржи један бинарни операцијски знак, који ћемо означавати двема вертикалним цртама $|\ |$ (између којих долазе аргументи), и два тернарна знака које ћемо означавати са $\angle$ и $\triangle$ (и који очекују три аргумента са десне стране). Нека је T_{cong} теорија чије су аксиоме универзална затворења[174] следећих формула:

γ_1 $|xy| = |yx|$,

γ_2 $\angle xyz = \angle zyx$,

γ_3 $\triangle xyz = \triangle uvw \Rightarrow |xy| = |uv| \wedge |yz| = |vw| \wedge |zx| = |wu|$,

γ_4 $\triangle xyz = \triangle uvw \Rightarrow \angle xyz = \angle uvw \wedge \angle yzx = \angle vwu \wedge \angle zxy = \angle wuv$,

γ_5 $|xy| = |uv| \wedge \angle xyz = \angle uvw \wedge |yz| = |vw| \Rightarrow \triangle xyz = \triangle uvw$.

Доказаћемо

$$T_{\mathrm{cong}} \vdash |ab| = |ac| \Rightarrow \angle abc = \angle acb.$$

Према правилу ($\Rightarrow_{\mathrm{U}}$), доказивање жељеног секвента сводимо на

$$T_{\mathrm{cong}}, |ab| = |ac| \vdash \angle abc = \angle acb.$$

Дакле, скуп претпоставки Γ садржи γ_1, γ_2, γ_3, γ_4, γ_5 и $|ab| = |ac|$.

1. $|ab| = |ac|$ — претпоставка, тј. (ax)
2. $|ac| = |ab|$ — из 1 према ($=_{\mathrm{S}}$)
3. $|ab| = |ba|$ — активирањем γ_1 правилом ($\forall_{\mathrm{E}}$) при $[x/a]$, $[y/b]$
4. $|ba| = |ab|$ — из 3 према ($=_{\mathrm{S}}$)
5. $|ba| = |ac|$ — из 4, 1 према ($=_{\mathrm{T}}$)
6. $|ac| = |ca|$ — активирањем γ_1 правилом ($\forall_{\mathrm{E}}$) при $[x/a]$, $[y/c]$
7. $|ba| = |ca|$ — из 5, 6 према ($=_{\mathrm{T}}$)
8. $\angle bac = \angle cab$ — активирањем γ_2 правилом ($\forall_{\mathrm{E}}$) при $[x/b]$, $[y/a]$, $[z/c]$
9. $|ba| = |ca| \wedge \angle bac = \angle cab \wedge |ac| = |ab|$ — из 7, 8, 2 применом ($\wedge_{\mathrm{U}}$) два пута
10. $|ba| = |ca| \wedge \angle bac = \angle cab \wedge |ac| = |ab| \Rightarrow \triangle bac = \triangle cab$ — активирањем γ_5 правилом ($\forall_{\mathrm{E}}$) при $[x/b]$, $[y/a]$, $[z/c]$, $[u/c]$, $[v/a]$, $[z/b]$
11. $\triangle bac = \triangle cab$ — из 9, 10 према ($\Rightarrow_{\mathrm{E}}$)
12. $\triangle cab = \triangle bac$ — из 11 према ($=_{\mathrm{S}}$)
13. $\triangle cab = \triangle bac \Rightarrow \angle cab = \angle bac \wedge \angle abc = \angle acb \wedge \angle bca = \angle cba$, — активирањем γ_4 правилом ($\forall_{\mathrm{E}}$) при $[x/c]$, $[y/a]$, $[z/b]$, $[u/b]$, $[v/a]$, $[w/c]$
14. $\angle cab = \angle bac \wedge \angle abc = \angle acb \wedge \angle bca = \angle cba$ — из 12, 13 према ($\Rightarrow_{\mathrm{E}}$)
15. $\angle abc = \angle acb$ — из 14 према ($\wedge^{\mathrm{l}}_{\mathrm{E}}$) и ($\wedge^{\mathrm{d}}_{\mathrm{E}}$).

[174] Универзално затворење формуле $\alpha(x_1, \ldots, x_k)$ јесте реченица $\forall x_1 \ldots \forall x_k \alpha(x_1, \ldots, x_k)$.

Пример 59. Занимљиву илустрацију уведених логичких концепата представља популарна игра Судоку: 9×9 табелу, која је подељена и на девет 3×3 блокова, као на слици десно, треба попунити бројевима од 1 до 9 тако да се сваки број појављује тачно једном у свакој колони, свакој врсти и сваком 3×3 блоку. Иницијално табела је делимично попуњена тако да се на јединствен начин може завршити. Основне идеје сасвим су сличне ситуацији из Примера 30, на страни 72.

	1	2	3	4	5	6	7	8	9
1	8								
2			3	6					
3		7			9		2		
4		5				7			
5					4	5	7		
6				1				3	
7			1					6	8
8			8	5				1	
9		9					4		

Правила игре описаћемо на вокабулару који чини један релацијски симбол $<$, један операцијски симбол $*$ и симболи бројева од 1 до 9. Значења ових симбола треба да одреде одговарајућу структуру над $\{1,2,3,4,5,6,7,8,9\}$, при чему:

• бројеви означавају врсте, одн. колоне табеле;

• релација $<$ одређује поредак међу колонама, одн. врстама; $x < y$ значи: *колона* x *је лево од колоне* y, тј. *врста* x *је изнад врсте* y;

• операција $*$ одређује садржај поља; $x * y = z$ значи: *у поље* (x, y) *уписан је број* z, при чему прва координата x означава врсту у којој се поље налази, а друга координата y колону у којој се поље налази.

Почетни садржај појединих поља одређује следећи списак (атомских) једнакости, (AT):
$1*1=8, 2*3=3, 2*4=6, 3*2=7, 3*5=9, 3*7=2, 4*2=5,$
$4*6=7, 5*5=4, 5*6=5, 5*7=7, 6*4=1, 6*8=3, 7*3=1,$
$7*8=6, 7*9=8, 8*3=8, 8*4=5, 8*8=1, 9*2=9, 9*7=4.$

Поредак колона, одн. врста је заправо релација строгог линеарног уређења бројева од 1 до 9:
(U1) $\forall x \neg(x < x)$
(U2) $\forall x \forall y\, (x < y \Rightarrow \neg(y < x))$
(U3) $\forall x \forall y \forall z\, (x < y \land y < z \Rightarrow x < z)$
(U4) $1 < 2 \land 2 < 3 \land 3 < 4 \land 4 < 5 \land 5 < 6 \land 6 < 7 \land 7 < 8 \land 8 < 9$

Правила да се у свакој врсти, одн. свакој колони, сваки број појављује тачно једном формулишемо на следећи начин:
(SV) $\forall x \forall y \forall z\, (x * y = x * z \Rightarrow y = z)$
(SK) $\forall x \forall y \forall z\, (x * z = y * z \Rightarrow x = y)$

	1	2	3	4	5	6	7	8	9
1	8								
2			3	6					
3		7			9		2		
4		5				7			
5					4	5	7		
6				1				3	
7			1					6	8
8			8	5				1	
9		9					4		

Остаје још да изразимо правила која се односе на појединачне блокове 3×3. Да бисмо олакшали читање, блокове означамо B11, B12, B13, B21, B22, B23, B31, B32, B33.
(B11) $\forall x \forall y \forall u \forall v(x < 4 \land y < 4 \land u < 4 \land v < 4 \land x * u = y * v \Rightarrow x = y \land u = v)$
(B22) $\forall x \forall y \forall u \forall v(3 < x \land x < 7 \land 3 < y \land y < 7 \land$
$\land 3 < u \land u < 7 \land 3 < v \land v < 7 \land x * u = y * v \Rightarrow x = y \land u = v)$
(B33) $\forall x \forall y \forall u \forall v(6 < x \land 6 < y \land 6 < u \land 6 < v \land x * u = y * v \Rightarrow x = y \land u = v)$
(B23) $\forall x \forall y \forall u \forall v(6 < x \land 6 < y \land 3 < u \land u < 7 \land 3 < v \land v < 7 \land x * u = y * v \Rightarrow x = y \land u = v)$
Корисно је запазити да су формуле за преостале блокове последице већ написаних својстава. Узимајући у обзир све ове претпоставке (AT) – (B23) изводимо читаво решење: $1 * 2 = 1$, $1 * 3 = 2$, $1 * 4 = 7$ итд.

Доста важних математичких истраживања и нових математичких области је настало управо због немогућности да се извесна тврђења докажу из неких датих претпоставки. Историја математике је пуна потрага за доказима, за које се испоставило да не постоје. Ипак, из тих безнадежних потрага за доказима често су се рађале сасвим нове математичке теорије. Илустрације ради, наводимо један занимљив проблем који се односи на HSI-алгебре

поменуте на почетку овог поглавља. Тарски је крајем 60-их година прошлог века поставио проблем који је данас познат као Тарскијев средњошколски проблем: *Да ли се из HSI теорије може извести сваки идентитет који је тачан у* $(\mathbb{N}^+, +, \cdot, \uparrow, 1)$? Британски математичар Алекс Вилки је 1980. године дао негативан одговор тако што је показао да је идентитет

$$\big((1+x)^y + (1+x+x^2)^y\big)^x \cdot \big((1+x^3)^x + (1+x^2+x^4)^x\big)^y$$
$$= \big((1+x)^x + (1+x+x^2)^x\big)^y \cdot \big((1+x^3)^y + (1+x^2+x^4)^y\big)^x$$

тачан у $(\mathbb{N}^+, +, \cdot, \uparrow, 1)$, али није последица HSI теорије. Тарскијев проблем и Вилкијево решење покренули су разне, још увек актуелне правце истраживања HSI алгебри.

$$(HSI)\ \begin{cases} x+y=y+x \\ (x+(y+z)=(x+y)+z \\ x\cdot 1=x \\ x\cdot y=y\cdot x \\ x\cdot(y\cdot z)=(x\cdot y)\cdot z \\ x\cdot(y+z)=x\cdot y+x\cdot z \\ x^1=x \\ 1^x=1 \\ x^{y+z}=x^y\cdot x^z \\ (x\cdot y)^z=x^z\cdot y^z \\ (x^y)^z=x^{y\cdot z} \end{cases}$$

▼ Задаци и додаци

1. На вокабулару структуре **N** дате су формуле:
- $\alpha(x,y)$ је $\neg x=0 \land \neg y=0 \land \exists z\,(x\cdot z=y)$
- $\beta(x)$ је $0'' \leqslant x \land \exists y \exists z\,(x=y\cdot z \Rightarrow y=1 \lor z=1)$
- $\gamma(x,y)$ је $\exists z(x+(z+z)=y \lor y+(z+z)=x)$.

Одредити, ако постоје, вредности променљивих за које је формула тачна, и вредности променљивих за које је формула нетачна.

2. Нека је R бинарни релацијски симбол. Уписати знак $\times$ у квадратић испред структуре у којој је тачна следећа реченица:

$$\exists x \exists y \exists z\,(R(x,y) \land R(z,y) \land R(x,z) \land \neg R(z,x))?$$

☐ $(\mathbb{N}^+, R^{\mathbf{N}})$, где је $R^{\mathbf{N}} = \{(m,m+1) \mid m \in \mathbb{N}^+\}$
☐ $(\mathbb{N}^+, R^{\mathbf{N}})$, где је $R^{\mathbf{N}} = \{(m,m+k) \mid m,k \in \mathbb{N}^+\}$
☐ $(\mathbb{N}^+, R^{\mathbf{N}})$, где је $R^{\mathbf{N}} = \{(m,mk) \mid m,k \in \mathbb{N}^+\}$

3. Нека је R бинарни релацијски симбол. Уписати знак $\times$ у квадратић испред структуре у којој је тачна следећа реченица:

$$\forall x \exists y \exists z\,(R(x,y) \land R(z,y) \land (R(x,z) \Rightarrow R(z,x)))?$$

☐ $(\mathbb{N}^+, R^{\mathbf{N}})$, где је $R^{\mathbf{N}} = \{(m,m+1) \mid m \in \mathbb{N}^+\}$
☐ $(\mathbb{N}^+, R^{\mathbf{N}})$, где је $R^{\mathbf{N}} = \{(m,m+k) \mid m \in \mathbb{N}^+, k \in \mathbb{N}\}$
☐ $(\mathbb{N}^+, R^{\mathbf{N}})$, где је $R^{\mathbf{N}} = \{(m,2m) \mid m \in \mathbb{N}^+\}$

4. Уписати знак $\times$ у квадратић испред реченице која је тачна у структури $(\mathbb{N}, \leqslant, ', +, \cdot, 0)$:
☐ $\forall x \forall y \forall z (x\cdot y=x\cdot z \Rightarrow y=z)$
☐ $\exists x\,(x\cdot x=x'')$
☐ $\forall x \forall y \exists z (x=y \lor x+z=y \lor y+z=x)$

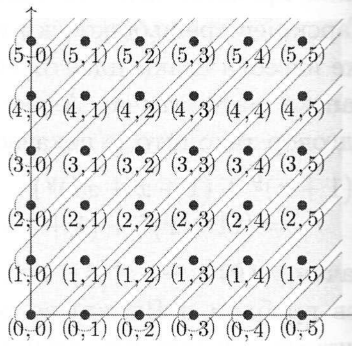
5. На вокабулару структуре $(\mathbb{N}^+, +, \cdot, 1)$ саставити формулу:
(а) $\alpha(x)$ која дефинише скуп парних бројева, тј. таква да је $\alpha(n)$ тачно у датој структури акко је n паран број;
(б) $\beta(x)$ која дефинише скуп простих бројева, тј. таква да је $\beta(n)$ тачно у датој структури акко је n прост број;
(в) $\gamma(x,y)$ која дефинише бинарну релацију '*дељивост*', тј. $\gamma(m,n)$ је тачно акко $m \mid n$;
(г) $\delta(x,y)$ која дефинише бинарну релацију '*узајамно прости*', тј.

$\delta(m,n)$ је тачно акко су m и n узајамно прости;
(д) $\eta(x,y,z)$ такву да је $\eta(k,m,n)$ тачно акко је $n = \text{nzd}(k,m)$.

6. (а) На скупу $\mathbb{N}\times\mathbb{N}$ дефинисана је релација $\sim$:

$$(a,b)\sim(c,d) \overset{\text{def}}{\Leftrightarrow} a+d=b+c.$$

Доказати да је $\sim$ релација еквиваленције.
(б) Ако је $(a,b)\sim(a_1,b_1)$ и $(c,d)\sim(c_1,d_1)$, доказати да је:
- $(a+c,b+d)\sim(a_1+c_1,b_1+d_1)$;
- $(ad+bc,ac+bd)\sim(a_1d_1+b_1c_1,a_1c_1+b_1d_1)$
- $(b,a)\sim(b_1,a_1)$.



Додатак

Релација $\sim$ из задатка 6 представља полазиште за конструкцију целих бројева. Конструкција је сасвим аналогна увођењу скупа $\mathbb{Q}_{\geqslant 0}$. Количнички скуп $\mathbb{N}\times\mathbb{N}/\sim$ називамо скупом целих бројева и означавамо $\mathbb{Z}$. Класа $[(a,b)]_\sim$ репрезентује решење једначине $a+x=b$, где су a и b параметри из $\mathbb{N}$.

Сабирање и множење целих бројева, $+_\mathbb{Z}, \cdot_\mathbb{Z} : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ дефинишемо једнакостима:

$$[(a,b)]_\sim +_\mathbb{Z} [(c,d)]_\sim \overset{\text{def}}{=} [(a+c,b+d)]_\sim, \quad [(a,b)]_\sim \cdot_\mathbb{Z} [(c,d)]_\sim \overset{\text{def}}{=} [(ad+bc,ac+bd)]_\sim.$$

Унарну операцију *супротан број* $-:\mathbb{Z}\to\mathbb{Z}$,

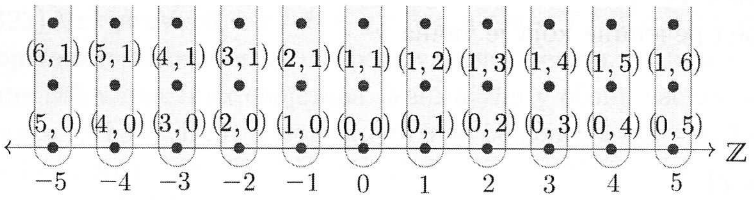
$$-[(a,b)]_\sim \overset{\text{def}}{=} [(b,a)]_\sim.$$

Бинарну релацију $\leqslant_\mathbb{Z}$ уводимо на следећи начин:

$$[(a,b)]_\sim \leqslant_\mathbb{Z} [(c,d)]_\sim \overset{\text{def}}{\Leftrightarrow} b+c\leqslant a+d,$$

где је $\leqslant$ уређење природних бројева. Веома је једноставно доказати коректност ове дефиниције, тј. да из $(a,b)\sim(a_1,b_1)$ и $(c,d)\sim(c_1,d_1)$, следи: $[(a,b)]_\sim \leqslant_\mathbb{Z} [(c,d)]_\sim$ акко $[(a_1,b_1)]_\sim \leqslant_\mathbb{Z} [(c_1,d_1)]_\sim$.

За сваки природан број a:
- класу $[(0,a)]_\sim$ краће означавамо a;
- класу $[(a,0)]_\sim$ краће означавамо $-a$.



---

7. Доказати да за произвољне $x,y,z\in\mathbb{Z}$:

$x+(y+z)=(x+y)+z$	$x\cdot(y\cdot z)=(x\cdot y)\cdot z$
$x+y=y+x$	$x\cdot y=y\cdot x$
$x+0=x$	$x\cdot 1=x,\ x\cdot 0=0$
$x+(-x)=0$	$x\cdot(y+z)=x\cdot y+x\cdot z$
$x\leqslant x$	$x\leqslant y\wedge y\leqslant x\Rightarrow x=y$
$x\leqslant y\wedge y\leqslant z\Rightarrow x\leqslant z$	$x\leqslant y\vee y\leqslant x$
$x\leqslant y\Rightarrow x+z\leqslant y+z$	$x\leqslant y\wedge 0\leqslant z\Rightarrow x\cdot z\leqslant y\cdot z$

8. [179] (а) На скупу $\mathbb{Z} \times \mathbb{N}^+$ је дефинисана бинарна релација:

$$(a, b) \approx (c, d) \overset{\text{def}}{\Leftrightarrow} a \cdot d = b \cdot c.$$

Доказати да је $\approx$ релација еквиваленције.

(б) На количничком скупу $\mathbb{Z} \times \mathbb{N}^+ / \approx$, који означавамо $\mathbb{Q}$, дефинисане су две бинарне операције, $+_{\mathbb{Q}}, \cdot_{\mathbb{Q}} : \mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$, једна унарна операција $-_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{Q}$, и бинарна релација $\leqslant_{\mathbb{Q}}$:

- $[(a, b)]_{\approx} +_{\mathbb{Q}} [(c, d)]_{\approx} \overset{\text{def}}{=} [(ad + bc, bd)]_{\approx}$;
- $[(a, b)]_{\approx} \cdot_{\mathbb{Q}} [(c, d)]_{\approx} \overset{\text{def}}{=} [(ac, bd)]_{\approx}$;
- $-_{\mathbb{Q}}[(a, b)]_{\approx} \overset{\text{def}}{=} [(a, -b)]_{\approx}$;
- $[(a, b)]_{\approx} \leqslant_{\mathbb{Q}} [(c, d)]_{\approx} \overset{\text{def}}{\Leftrightarrow} bd \leqslant ac$.

Доказати да су ове операције и релација добро дефинисане.

[179] У овом задатку је описана конструкција рационалних бројева.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

$$-\frac{a}{b} = \frac{-a}{b}$$

$$\frac{a}{b} \leqslant_{\mathbb{Q}} \frac{c}{d} \Leftrightarrow ad \leqslant bc$$

9. Доказати да за произвољне $x, y, z \in \mathbb{Q}$:

$x + (y + z) = (x + y) + z$	$x \cdot (y \cdot z) = (x \cdot y) \cdot z$
$x + y = y + x$	$x \cdot y = y \cdot x$
$x + 0 = x$	$x \cdot 1 = x,\ x \cdot 0 = 0$
$x + (-x) = 0$	$x \cdot (y + z) = x \cdot y + x \cdot z$

$$(*)\quad x \neq 0 \Rightarrow (\exists u \in \mathbb{Q})\, x \cdot u = 1$$

$x \leqslant x$	$x \leqslant y \land y \leqslant x \Rightarrow x = y$
$x \leqslant y \land y \leqslant z \Rightarrow x \leqslant z$	$x \leqslant y \lor y \leqslant x$
$x \leqslant y \Rightarrow x + z \leqslant y + z$	$x \leqslant y \land 0 \leqslant z \Rightarrow x \cdot z \leqslant y \cdot z$

10. Испитати тачност следећих реченица у структурама (истог вокабулара) $\mathbf{Z} = (\mathbb{Z}, \leqslant, +, \cdot, -, 0, 1)$ и $\mathbf{Q} = (\mathbb{Q}, \leqslant, +, \cdot, -, 0, 1)$:

(а) $\forall x \forall y\, (0 \leqslant x \land x \cdot y = 1 \Rightarrow x = 1 \land y = 1)$

(б) $\forall x \exists y\, (y + y = x \cdot y)$

(в) $\forall x \exists y\, (y \cdot y + x \cdot y = x + 1)$

(г) $\forall x \exists y\, (y \cdot (y + 1) = x + 1)$

(ђ) $\forall x \forall y\, (x + x \leqslant y + y \Rightarrow x \leqslant y)$

(е) $\forall x \forall y\, (x \cdot x \leqslant y \cdot y \Rightarrow x \leqslant y)$

11. Доказати:

$\forall x\, (f(x) = f(f(x))), \forall x \forall y\, (f(x) = f(y) \Rightarrow x = y) \vdash \forall z \exists x\, (f(x) = z)$

ДОДАТАК

Теорија група. Вокабулар група чини симбол једне бинарне операције, симбол једне унарне операције и симбол једне константе; често се у општем случају користе следећи симболи: $*$, $^{-1}$, e. Теорију група чине следеће реченице:

(A) $\forall x \forall y \forall z\, (x * (y * z) = (x * y) * z)$

(N) $\forall x\, (x * e = x)$

(I) $\forall x\, (x * x^{-1} = e)$

Група је свака структура $(G, *, ^{-1}, e)$ која задовољава наведене аксиоме. У наредним задацима наведено је неколико примера група.

---

12. Нека је S_X скуп свих бијекција (пермутација) скупа X. Доказати да је $(S_X, \circ, ^{-1}, \mathrm{id}_X)$ група.

13. Нека је S било који скуп. На скупу $\mathcal{P}(S)$ посматрајмо *симетричну разлику*: $X \triangle Y = (X \setminus Y) \cup (Y \setminus X)$ и нека је $\mathbf{I}$ краћа ознака за идентичку функцију скупа $\mathcal{P}(S)$: $\mathbf{I}(A) = A$, за $A \in \mathcal{P}(A)$. Доказати да је структура $(\mathcal{P}(S), \triangle, \mathbf{I}, \emptyset)$ група.

14. Дефинисати бар једну групу чији је домен скуп $\mathbb{N}$.

15. Ако је T_G теорија група[181], доказати:

$T_G, \forall x\,(x * x = e) \vdash \forall x \forall y\,(x * y = y * x)$

16. Нека је T теорија вокабулара $\{+, 0\}$:

$\forall x \forall y \forall z\,(x + (y + z) = (x + y) + z)$

$\forall x\,((x + 0 = x) \wedge (0 + x = x))$

$\forall x(\exists y(x + y = 0) \wedge \exists z(z + x = 0))$

Доказати:

(а) $T \vdash \forall x \forall y \forall z\,(x + y = x + z \Rightarrow y = z)$

(б) $T \vdash \forall x\,(\forall y(x + y = y) \Rightarrow x = 0)$

(в) $T \vdash \forall x \exists y \forall z\,((x + y = 0) \wedge (z + x = 0) \Rightarrow y = z)$

17. Нека је T_E теорија вокабулара који садржи само један бинарни релацијски симбол E:

$\forall x\, E(x, x)$

$\forall x \forall y\,(E(x, y) \Rightarrow E(y, x))$

$\forall x \forall y \forall z\,(E(x, y) \wedge E(y, z) \Rightarrow E(x, z))$

Доказати $T_E, \exists x(E(x, y) \wedge E(x, z)) \vdash \forall x(E(x, y) \Leftrightarrow E(x, z))$.

18. Ако је B бинарни релацијски симбол, доказати да ниједна од следећих формула није последица преостале две:

$\forall x \forall y \forall z\,(B(x, y) \wedge B(y, z) \Rightarrow B(x, z))$

$\forall x \forall y\,(B(x, y) \wedge B(y, x) \Rightarrow x = y)$

$\forall x \exists y\, B(x, y) \Rightarrow \exists y \forall x\, B(x, y)$

19. Нека су A и B унарни релацијски симболи, а f унарни операцијски симбол. Доказати:

(а) $\exists x \exists y\,(A(x) \wedge A(y) \wedge \neg(x = y)), \forall x \forall y\,(B(x) \wedge B(y) \Rightarrow x = y) \vdash \exists x\,(A(x) \wedge \neg B(x))$

(б) $\forall x \forall y\,(A(x) \wedge A(y) \Rightarrow x = y), \exists x\,(A(x) \wedge \neg B(x)) \vdash \forall x\,(B(x) \Rightarrow \neg A(x))$

(в) $\exists x\, A(x), \forall x\,(A(x) \Rightarrow B(f(x))), \forall x\, \neg(A(x) \wedge B(x)) \vdash \exists x \exists y\, \neg(x = y)$

20. Нека је f унарни операцијски симбол, а 0 и 1 симболи константи.

(а) Из претпоставки:

$\forall x\,(f(x) = 0 \vee f(x) = 1)$

$\exists x \exists y \exists z\,(\neg(x = y) \wedge \neg(y = z) \wedge \neg(z = x))$,

извести[182] формулу

$\exists x \exists y\,(\neg(x = y) \wedge f(x) = f(y))$.

(б) Из претпоставки:

$\forall x\,(f(f(x)) = x)$

$\forall x \forall y \forall z \forall u\,(x = y \vee x = z \vee x = u \vee y = z \vee y = u \vee z = u)$

$\exists x \exists y \exists z\,(\neg(x = y) \wedge \neg(y = z) \wedge \neg(z = x))$

извести формулу

$\exists v\, f(v) = v$.

[181] T_G чине следеће реченице:
$\forall x \forall y \forall z\,(x * (y * z) = (x * y) * z)$
$\forall x\,(x * e = x)$
$\forall x\,(x * x^{-1} = e)$

[182] Довољно је навести детаљан опис извођења тако да се на основу тог описа једноставно састављa формални доказ природном дедукцијом.

4.4. Квантификатор $\mathcal{U}$-скоро свуда

Увод. Рационални бројеви нису довољни да изразе резултате мерења дужине сваке дужи (еуклидске геометрије). Када је задата јединична дуж, познати поступак мерења подразумева прекривање дужи која се мери надовезивањем јединице мере и њених делова. Јединицу мере, и сваки њен део, увек делимо на исти број мањих делова. Чувени пример представља мерење дијагонале јединичног квадрата. Из геометрије је познато да је дужина дијагонале јединичног квадрата решење једначине $x^2 = 2$, као и да ова једначина нема решења у скупу $\mathbb{Q}_{\geqslant 0}$.

Не постоје природни бројеви a, b такви да је $\left(\frac{a}{b}\right)^2 = 2$, тј. да је $a^2 = 2b^2$.

Поступак мерења дијагонале квадрата његовом страницом генерише један низ ненегативних рационалних бројева. Користећи децималну поделу јединичне дужи (поделу на 10 једнаких делова) и децималне записе рационалних бројева, добијамо следеће процене:

- $1 < x < 2$, на основу $1^2 < x^2 = 2 < 2^2$
- $1,4 < x < 1,5$, на основу табеле

x	1,0	1,1	1,2	1,3	**1,4**	**1,5**	1,6	1,7	1,8	1,9	2,0
x^2	1,0	1,21	1,44	1,69	**1,96**	**2,25**	2,56	2,89	3,24	3,61	4

- $1,41 < x < 1,42$, на основу табеле

x	1,4	1,41	1,42	⋯
x^2	1,96	1,9881	2,0164	⋯

- $1,414 < x < 1,415$, јер је $1,999396 < x^2 < 2,002225$
- $1,4142 < x < 1,4143$, јер је $1,99996164 < x^2 < 2,00024449$
- $1,41421 < x < 1,41422$, јер је $1,9999899241 < x^2 < 2,0000182084$
- $1,414213 < x < 1,414214$, јер је $1,999998409369 < x^2 < 2,000001237796$

итд. Приказани поступак мерења дијагонале јединичног квадрата се не завршава. Узимајући, на пример, леве процене дужине дијагонале, уочамо низ рационалних бројева чији се чланови све мање међусобно разликују.

План

- Хиперрационални бројеви; реални бројеви
- Теорема компактности; коначна верзија Ремзијеве теореме

▼ Реални бројеви

Уводни пример показује да се низови ненегативних рационалних бројева појављују као резултати мерења. Покушај да се изгради нови скуп бројева (а самим тим структура над њим), довољно богат да се изразе резултати мерења дужи, природно је започети изградњом структуре над $\mathbb{Q}^{\mathbb{N}}$. Показаћемо како нам ултрафилтер омогућава да полазећи од низова рационалних бројева изградимо веома богату структуру у којој ћемо проучавати феномене у вези са мерењем. Та структура ће бити проширење структуре рационалних бројева.

$\mathbb{Q}^{\mathbb{N}}$ је скуп свих низова рационалних бројева.

Ако сваки рационалан број $q \in \mathbb{Q}$ идентификујемо са константним низом $(q, q, q, \ldots) \in \mathbb{Q}^{\mathbb{N}}$, уз запис $q \equiv (q, q, q, \ldots)$, скуп $\mathbb{Q}^{\mathbb{N}}$ можемо посматрати као проширење (надскуп) скупа $\mathbb{Q}$. Подразумева се да је једнакост међу низовима дефинисана по координатама:

$$(\star) \qquad (q_n) = (r_n) \Leftrightarrow (\forall n \in \mathbb{N})(q_n = r_n)$$

Сходно томе, на скупу $\mathbb{Q}^{\mathbb{N}}$ можемо дефинисати уређење и операције *по координатама*, 'поштујући' операције и уређење рационалних бројева:

$$(q_n) \leqslant (r_n) \overset{\text{def}}{\Leftrightarrow} (\forall n \in \mathbb{N})(q_n \leqslant r_n),\ (q_n) + (r_n) \overset{\text{def}}{=} (q_n + r_n),\ (q_n) \cdot (r_n) \overset{\text{def}}{=} (q_n \cdot r_n)$$

Међутим, са оваквим дефиницијама, престају да важе нека значајна својства рационалних бројева:

• уређење по координатама није линеарно; нпр. низови $(0, 1, 0, 1, \ldots)$ и $(1, 0, 1, 0, \ldots)$ нису упоредиви;

• низ различит од нуле не мора имати инверзни у односу на множење; нпр. за $(0, 1, 0, 1, \ldots) \neq (0, 0, 0, 0, \ldots) \equiv 0$ не постоји низ (q_n) такав да је $(0, 1, 0, 1, \ldots) \cdot (q_0, q_1, q_2, q_3, \ldots) = (1, 1, 1, 1, \ldots) \equiv 1$.

Важно запажање јесте да ћемо сачувати сва значајна својства рачунских операција и уређења рационалних бројева уколико уместо једнакости $(\star)$, уведемо следеће изједначавање:

$$(*) \qquad (q_n) =_{\mathcal{U}} (r_n) \Leftrightarrow (\mathcal{U}n)(q_n = r_n),$$

при чему је $\mathcal{U}$ ултрафилтер на $\mathbb{N}$ који проширује Фрешеов филтер[185]. Уместо да подразумевамо да су сви одговарајући чланови низова међусобно једнаки, захтевамо да су $\mathcal{U}$-скоро сви одговарајући чланови низова међусобно једнаки.

[185] Квантификатор $\mathcal{U}$-скоро сви је проширење квантификатора: *сви осим њих коначно много* (видети стране 140 и 141).

Лема 19. *Нека је $\mathcal{U}$ ултрафилтер на $\mathbb{N}$. Релација на $\mathbb{Q}^{\mathbb{N}}$ дефинисана са $(*)$ је релација еквиваленције.*

Доказ. Нека су (q_n), (r_n) и (s_n) произвољни низови.
(Р) Из $(\forall n \in \mathbb{N})(q_n = q_n)$, следи $(\mathcal{U}n)(q_n = q_n)$, тј. $(q_n) =_{\mathcal{U}} (q_n)$.
(С) Ако је $(q_n) =_{\mathcal{U}} (r_n)$, тј. $(\mathcal{U}n)(q_n = r_n)$, из $(\forall n \in \mathbb{N})(q_n = r_n \Rightarrow r_n = q_n)$ следи $(\mathcal{U}n)(r_n = q_n)$, тј. $(r_n) =_{\mathcal{U}} (q_n)$.
(Т) Нека је $(q_n) =_{\mathcal{U}} (r_n)$ и $(r_n) =_{\mathcal{U}} (s_n)$, тј. $(\mathcal{U}n)(q_n = r_n)$ и

$(\mathcal{U}n)(r_n = s_n)$. Из $(\forall n \in \mathbb{N})(q_n = r_n \wedge r_n = s_n \Rightarrow q_n = s_n)$ следи $(\mathcal{U}n)(q_n = s_n)$ тј. $(q_n) =_{\mathcal{U}} (s_n)$. □

Класу еквиваленције $[(q_n)]_{\mathcal{U}}$ краће означавамо $\langle q_n \rangle$ и називамо **хиперрационалан број**. Дакле,

$$\langle q_n \rangle = \langle r_n \rangle \;\Leftrightarrow\; (q_n) =_{\mathcal{U}} (r_n).$$

Количнички скуп $\mathbb{Q}^{\mathbb{N}} / =_{\mathcal{U}}$ означавамо $^*\mathbb{Q}$. Очекивано, рационалан број q идентификујемо са $\langle q, q, q, \ldots \rangle$. Дефинишимо на скупу $^*\mathbb{Q}$ једну релацију и две операције:

$\langle q_n \rangle \leqslant^* \langle r_n \rangle \overset{\text{def}}{\Leftrightarrow} (\mathcal{U}n)(q_n \leqslant r_n)$, $\langle q_n \rangle +^* \langle r_n \rangle \overset{\text{def}}{=} \langle q_n + r_n \rangle$, $\langle q_n \rangle \cdot^* \langle r_n \rangle \overset{\text{def}}{=} \langle q_n \cdot r_n \rangle$.

Следећа лема, чији доказ остављамо за вежбу, потврђује коректност претходних дефиниција.

Лема 20. *Ако је* $\langle q_n \rangle = \langle s_n \rangle$ *и* $\langle r_n \rangle = \langle t_n \rangle$, *онда је*
$\langle q_n \rangle \leqslant^* \langle r_n \rangle \;\Leftrightarrow\; \langle s_n \rangle \leqslant^* \langle t_n \rangle, \langle q_n + r_n \rangle = \langle s_n + t_n \rangle, \langle q_n \cdot r_n \rangle = \langle s_n \cdot t_n \rangle$.

Једноставно се проверава да $\leqslant^*$, $+^*$, $\cdot^*$ наслеђују сва важна својства уређења $\leqslant$ и операција $+$ и $\cdot$ рационалних бројева. На пример:
- ако је $\langle q_n \rangle \leqslant^* \langle r_n \rangle$ и $\langle r_n \rangle \leqslant^* \langle q_n \rangle$, онда је $\langle q_n \rangle = \langle r_n \rangle$. Заиста, из $(\mathcal{U}n)(q_n \leqslant r_n)$ и $(\mathcal{U}n)(r_n \leqslant q_n)$, користећи антисиметричност уређења скупа $\mathbb{Q}$: $(\forall n \in \mathbb{N})(q_n \leqslant r_n \wedge r_n \leqslant q_n \Rightarrow q_n = r_n)$, закључујемо $(\mathcal{U}n)(q_n = r_n)$, тј. $\langle q_n \rangle = \langle r_n \rangle$.
- за све $\langle q_n \rangle$ и $\langle r_n \rangle$, $\langle q_n \rangle +^* \langle r_n \rangle = \langle r_n \rangle +^* \langle q_n \rangle$. Узимајући у обзир дефиницију сабирања хиперрационалних бројева, траба доказати да је $\langle q_n + r_n \rangle = \langle r_n + q_n \rangle$, тј. $(\mathcal{U}n)\,(q_n + r_n = r_n + q_n)$, али то је једноставна последица чињенице $(\forall n \in \mathbb{N})\,(q_n + r_n = r_n + q_n)$.

Очигледно је да можемо изоставити $*$ из ознака операција и уређења, јер се поштују операције и уређење рационалних бројева.

Из уводног примера видимо да поступак мерења генерише један (бесконачни) децимални број. Ултрафилтер омогућава да се сваком ограниченом низу придружи један децимални број.

Низ (q_n) је **ограничен** ако постоји позитиван рационалан број M такав да је $|q_n| < M$, за све $n \in \mathbb{N}$. Помоћу ултрафилтера сваком ограниченом низу придружујемо тзв. *децимални развој*:
- сваки члан низа (q_n) припада неком од коначно много интервала

$$[-M, -M+1), \ldots, [0,1), \ldots, [M-1, M),$$

и према уопштеном Дирихлеовом принципу, само једном од ових интервала припадају $\mathcal{U}$-скоро сви чланови низа; нека је то интервал $[d_0, d_0+1)$; дакле, $(\mathcal{U}n)\; d_0 \leqslant q_n < d_0 + \frac{d_1}{10}$;
- ако интервал $[d_0, d_0+1)$ поделимо на 10 једнаких делова:
$\left[d_0, d_0 + \frac{1}{10}\right), \left[d_0 + \frac{1}{10}, d_0 + \frac{2}{10}\right), \left[d_0 + \frac{2}{10}, d_0 + \frac{3}{10}\right), \ldots, \left[d_0 + \frac{9}{10}, d_0 + 1\right)$
постојаће само један део коме ће припадати $\mathcal{U}$-скоро сви чланови низа; нека је то $\left[d_0 + \frac{d_1}{10}, d_0 + \frac{d_1+1}{10}\right)$, за неко d_1, $0 \leqslant d_1 < 10$; дакле, $(\mathcal{U}n)\; d_0 + \frac{d_1}{10} \leqslant q_n < d_0 + \frac{d_1}{10} + \frac{d_2}{100}$;

• ако интервал $\left[d_0 + \frac{d_1}{10}, d_0 + \frac{d_1+1}{10}\right)$, поделимо на 10 једнаких делова, постојаће само један део коме ће припадати $\mathcal{U}$-скоро сви чланови низа; нека је то $\left[d_0 + \frac{d_1}{10} + \frac{d_2}{100}, d_0 + \frac{d_1}{10} + \frac{d_2+1}{100}\right)$, $0 \leqslant d_2 < 10$; итд. Низ рационалних бројева, добијен на овај начин

$$\overline{q}_0 = d_0, \overline{q}_1 = d_0 + \frac{d_1}{10}, \overline{q}_2 = d_0 + \frac{d_1}{10} + \frac{d_2}{100}, \ldots$$

називаћемо **децимални развој** низа (q_n). Низ $(\overline{q}_n)$ краће представљамо на следећи начин $d_0 + 0, d_1 d_2 d_3 \ldots$, при чему је d_0 цео број који називамо *цели део* развоја, а сваки d_i из $\{0, 1, \ldots, 9\}$ називамо *децималом.* Корисно је уочити неједнакости:

$$\overline{q}_n \leqslant q_{n+k} < \overline{q}_n + \frac{1}{10^n}, \; n, k \geqslant 0$$

Различитим низовима могу одговарати исти децимални развоји. Генерално, идентификујемо децималне развоје свака два низа (q_n) и (r_n) таква да је:

$$(**) \qquad (\forall n \in \mathbb{N}) \left(|q_n - r_n| \leqslant \frac{1}{10^n}\right)$$

Услов $(**)$ задовољавају и децимални развоји којима одговарају записи $a_0, 999\ldots$ и $a_0 + 1$, као и записи

$$a_0, a_1 \ldots a_k 999 \ldots \text{ и } a_0, a_1 \ldots (a_k + 1)000 \ldots$$

при чему је $a_k \neq 9$, за неко $k > 0$. Сходно томе, наведене парове децималних записа сматрамо једнаким. Увек ћемо предност давати записима који се завршавају низом нула. По договору, ако су све децимале, почев од неког места једнаке 0, онда их не записујемо. Посебно, развој чије су све децимале једанаке 0, идентификујемо са целим бројем који представља цели део тог развоја. Најзад, запис $0 + 0, d_1 d_2 d_3 \ldots$ скраћено пишемо $0, d_1 d_2 d_3 \ldots$

Од посебног значаја је следећа лема.

Лема 21. *За свака два ограничена низа (q_n) и (r_n):*

$$(\forall \varepsilon \in \mathbb{Q}_{>0})(\mathcal{U}n)(|q_n - r_n| < \varepsilon) \text{ акко } (\forall n \in \mathbb{N})\,(\overline{q}_n = \overline{r}_n).$$

Доказ. $(\Rightarrow)$ Претпоставимо $(\forall \varepsilon \in \mathbb{Q}_{>0})(\mathcal{U}n)(|q_n - r_n| < \varepsilon)$ и да је $\overline{q}_k \neq \overline{r}_k$, за неко k. Без губљења општости, можемо додатно претпоставити да је $\overline{q}_k > \overline{r}_k$. Тада је $\overline{q}_k - \overline{r}_k > \frac{1}{10^k}$. Нека је $\varepsilon_0 = \overline{q}_k - \overline{r}_k - \frac{1}{10^k} > 0$. За свако $n \geqslant k$, важе неједнакости:

$$\overline{r}_k \leqslant r_n < \overline{r}_k + \frac{1}{10^k} < \overline{q}_k \leqslant q_n < \overline{q}_k + \frac{1}{10^k},$$

одакле следи да је $q_n - r_n > \varepsilon_0$. Пошто $\mathcal{U}$ садржи све ко-коначне скупове, закључујемо $(\mathcal{U}n)(|q_n - r_n| > \varepsilon_0)$ што је супротно полазној претпоставци.
$(\Leftarrow)$ Претпоставимо да $(\forall n \in \mathbb{N})\,(\overline{q}_n = \overline{r}_n)$. Нека је $\varepsilon > 0$ произвољно и k природан број такав да је $\frac{2}{10^k} < \varepsilon$. Није тешко показати

да овакав природан број k постоји. У наставку доказа биће јасно зашто је на овај начин изабран број k. За сваки природан број $n \geqslant k$, из $\overline{q}_n = \overline{r}_n$ следи:

$$\begin{aligned} |q_n - r_n| &= |q_n - \overline{q}_n - r_n + \overline{r}_n| \\ &= |q_n - \overline{q}_n + (\overline{r}_n - r_n)| \\ &\leqslant |q_n - \overline{q}_n| + |r_n - \overline{r}_n| \\ &\leqslant \frac{1}{10^n} + \frac{1}{10^n} = \frac{2}{10^n} \leqslant \frac{2}{10^k} < \varepsilon \end{aligned}$$

Дакле, $(\mathcal{U}n)(|q_n - r_n| < \varepsilon)$. □

За произвољне рационалне бројеве x, y важи тзв. *неједнакост троугла*: $|x + y| \leqslant |x| + |y|$.

Пример 60. Према претходној леми закључујемо да низовима:

$$\left(1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right), \left(-1, -\frac{1}{2^2}, -\frac{1}{3^2}, -\frac{1}{4^2}, \ldots\right), \left(1, -\frac{1}{2}, \frac{1}{2^2}, -\frac{1}{2^3}, \ldots\right)$$

одговара децимални запис: $0.0000\ldots$, тј. 0. Наиме, сви наведени низови задовољавају следећу особину: *за свако* $\varepsilon > 0$, *интервал* $(-\varepsilon, \varepsilon)$ *садржи све чланове низа, осим можда коначно много њих*, тј. увек је изван интервала само коначно много чланова. Како је ултрафилтер $\mathcal{U}$ проширење Фрешеовог филтера, закључујемо да сваки од интервала садржи $\mathcal{U}$-скоро све чланове низа.

Ако Фрешеов филтер $\mathcal{F}^\infty$ посматрамо као квантификатор, онда уочену особину можемо записати и на следећи начин:

$$(\mathcal{F}^\infty n)\ (|q_n - 0| < \varepsilon)\,.$$

Посебно издвајамо низове који имају особину истакнуту у претходном примеру. Низ (e_n) је **нула-низ** ако за сваки позитиван рационалан број ε, интервал $(-\varepsilon, \varepsilon)$ садржи све чланове низа, осим можда коначно много њих. Свим нула-низовима одговара децимални запис $0.000\ldots$, тј. 0.

Разматрања о низовима рационалних бројева природно преводимо у контекст богате структуре хиперрационалних бројева. Уведене врсте низова (ограничени низови и нула-низови) одређују посебне врсте хиперрационалних бројева. Да бисмо поједноставили записивање формула, уместо $\exists M \in \mathbb{Q}_{>0}$ и $\forall \varepsilon \in \mathbb{Q}_{>0}$ краће пишемо $\exists M$ и $\forall \varepsilon$ подразумевајући да су промењиве уз класичне квантификаторе ограничене на скуп $\mathbb{Q}_{>0}$.

Низ рационалних бројева (q_n) је:	Хиперрационалан број $\langle q_n \rangle$ је:
• **ограничен** ако	• **коначан** ако
$\exists M (\forall n \in \mathbb{N})\ (\lvert q_n\rvert < M)$;	$\exists M (\mathcal{U} n)\ (\lvert q_n\rvert < M)$;
• **нула низ** ако	• **инфинитезимала** ако
$\forall \varepsilon (\exists n_0 \in \mathbb{N})(\forall n \in [n_0, +\infty)_{\mathbb{N}})\ (\lvert q_n\rvert < \varepsilon)$.	$\forall \varepsilon (\mathcal{U} n)\ (\lvert q_n\rvert < \varepsilon)$.

Јасно, сваки ограничен низ (q_n) одређује један коначни хиперрационалан број $\langle q_n \rangle$. У извесном смислу и обрнуто је тачно. У општем случају, ако је $\langle q_n \rangle$ коначан хиперрационалан број, онда низ (q_n) не мора бити ограничен; али увек можемо изабрати представника класе $\langle q_n \rangle$ који јесте ограничен. Ако је $\langle q_n \rangle$ коначан, онда постоји $M > 0$ такав да је $(\mathcal{U} n)\ (|q_n| < M)$. Нека је $S = \{n \in \mathbb{N} \mid |q_n| < M\} \in \mathcal{U}$, и (r_n) низ дефинисан на следећи

начин:

$$r_n = \begin{cases} q_n, & n \in S, \\ 0, & n \notin S. \end{cases}$$

Очигледно је (r_n) ограничен низ и $\langle q_n \rangle = \langle r_n \rangle$. Јасно, сваки нула-низ одређује једну инфинитезималу, и обрнуто: за сваку инфинитезималу $\langle e_n \rangle$ постоји нула-низ (f_n) такав да је $\langle e_n \rangle = \langle f_n \rangle$.

Лема 22. *1) Збир и производ два коначна хиперрационална броја такође су коначни хиперрационални бројеви. 2) Збир и производ две инфинитезимале такође су инфинитезимале. 3) Производ инфинитезимале и коначног броја је инфинитезимала.*

Доказ. Доказујемо само 3). Нека је $\langle q_n \rangle$ коначан број, а $\langle e_n \rangle$ инфинитезимала: (1) $\exists M (\mathcal{U} n)\ (|q_n| < M)$ и (2) $\forall \varepsilon (\mathcal{U} n)\ (|e_n| < \varepsilon)$. Како је $\langle e_n \rangle \cdot \langle q_n \rangle = \langle e_n q_n \rangle$, треба доказати $\forall \varepsilon (\mathcal{U} n)\ (|e_n q_n| < \varepsilon)$.

Нека је $\varepsilon > 0$ произвољан рационалан број. Ако је M позитиван рационалан број такав да је $(\mathcal{U} n)\ (|q_n| < M)$, из формуле (2)[188] добијамо $(\mathcal{U} n)\ (|e_n| < \varepsilon M^{-1})$. Најзад, из $(\mathcal{U} n)\ (|q_n| < M)$ и $(\mathcal{U} n)\ (|e_n| < \varepsilon M^{-1})$ следи $(\mathcal{U} n)\ (|e_n q_n| < \varepsilon M^{-1} M = \varepsilon)$. □

[188] Реч је о примени правила $(\forall \varepsilon_E)$ на формулу (2) $\forall \varepsilon (\mathcal{U} n)\ (|e_n| < \varepsilon)$, са заменом универзално квантификоване променљиве ε изразом εM^{-1}.

Сваком коначном хиперрационалном броју $\langle q_n \rangle$ одговара јединствен децимални развој $d_0 + 0, d_1 d_2 \ldots$ (одн. $(\overline{q}_n)$) који називамо **стандардним делом** хиперрационалног броја $\langle q_n \rangle$; пишемо $\mathrm{st}\langle q_n \rangle = d_0 + 0, d_1 d_2 \ldots$ Очигледна је добра дефинисаност: ако је $\langle q_n \rangle = \langle r_n \rangle$, за неке ограничене низове (q_n) и (r_n), из $(\mathcal{U} n)(q_n = r_n)$, према леми 21, следи да за свако n, $\overline{q}_n = \overline{r}_n$. Директна последица Леме 21 је следеће тврђење.

Последица 6. *Нека су q и r коначни хиперрационални бројеви. Тада је $\mathrm{st}(q) = \mathrm{st}(r)$ акко је $q - r$ инфинитезимала.*

Сваки децимални развој $d_0 + 0, d_1 d_2 \ldots$, где је $d_0 \in \mathbb{Z}$, и $d_i \in \{0, 1, \ldots, 9\}$, $i \geqslant 1$, тј. одговарајући ограничени низ $(\overline{q}_n)$:

$$\overline{q}_0 = d_0,\ \overline{q}_n = d_0 + \frac{d_1}{10^1} + \cdots + \frac{d_n}{10^n}, n \geqslant 1.$$

одређује један коначан хиперрационалан број $\langle \overline{q}_n \rangle$, при чему је

$$\mathrm{st}(\langle \overline{q}_n \rangle) = (\overline{q}_n) = d_0 + 0, d_1 d_2 \ldots$$

Сваки (коначан) хиперрационалан број одређен децималним развојем називамо **реалан број**. Скуп свих реалних бројева обележавамо $\mathbb{R}$. Из претходних разматрања, следи важно запажање.

Лема 23. *Сваки коначан хиперрационалан број се може на јединствен начин представити као збир реалног броја и инфинитезимале.*

Скуп коначних хиперрационалних бројева означавамо ${}^*\mathbb{Q}_{\mathrm{fin}}$. Дакле, $\mathbb{R} \subseteq {}^*\mathbb{Q}_{\mathrm{fin}}$ и $\mathrm{st} : {}^*\mathbb{Q}_{\mathrm{fin}} \to \mathbb{R}$, при чему је $\mathrm{st}(a) = a$, за свако $a \in \mathbb{R}$. Овакво пресликавање st нам омогућава да и на $\mathbb{R}$ изградимо структуру истог типа као на ${}^*\mathbb{Q}$: за све $a, b \in \mathbb{R}$,

$$a +_{\mathbb{R}} b \stackrel{\mathrm{def}}{=} \mathrm{st}(a + b),\ a \cdot_{\mathbb{R}} b \stackrel{\mathrm{def}}{=} \mathrm{st}(a \cdot b).$$

За функцију $\mathrm{st} : \mathbb{Q}_{\mathrm{fin}} \to \mathbb{R}$ каже се и да је ретракција; а за скуп реалних бројева да је ретракт од ${}^*\mathbb{Q}_{\mathrm{fin}}$.

Реалне бројеве уређујемо поредећи лексикографски децималне развоје који их одређују:

$$a_0 + 0, a_1a_2a_3 \ldots <_{\mathbb{R}} b_0 + 0, b_1b_2b_3 \ldots$$

ако је $a_0 < b_0$ или постоји k такво да је $a_i = b_i$, за $i < k$ и $a_k < b_k$.

Лема 24. *Релација $\leqslant_{\mathbb{R}}$ је линеарно уређење на $\mathbb{R}$ и сваки одозго ограничен подскуп од $\mathbb{R}$ има најмање горње ограничење, тзв. супремум.*

Доказ. Једноставно се проверава да је $\leqslant_{\mathbb{R}}$ линеарно уређење на $\mathbb{R}$. Нека је D ограничен одозго подскуп од $\mathbb{R}$. Скуп D_0 који чине цели делови свих елемената из D ограничен је подскуп скупа $\mathbb{Z}$, што значи да постоји максималан цео број у D_0; нека је $d_0 = \max D_0 \in \mathbb{Z}$. Из скупа D даље издвајамо подскуп D_1 који чине сви развоји чији је цели део d_0. Ако је C_1 скуп свих првих децимала развоја из D_1, онда је $C_1 \subseteq \{0, 1, 2, \ldots, 9\}$; нека је $d_1 = \max C_1$. Индуктивно настављамо поступак: за свако k, из скупа D_k издвајамо подскуп D_{k+1} који чине сви развоји чија је k-та децимала d_k. Ако је C_{k+1} скуп свих $(k+1)$. децимала развоја из D_{k+1}, онда је $C_{k+1} \subseteq \{0, 1, 2, \ldots, 9\}$; нека је $d_{k+1} = \max C_{k+1}$. На овај начин добијамо децимални развој $d_0 + 0, d_1d_2 \ldots d_k$, тј. одговарајући реалан број, који је супремум скупа D. □

Теорема 47. *Нека су q и r произвољни коначни хиперрационални бројеви.*
1) $\mathrm{st}(q + r) = \mathrm{st}(q) +_{\mathbb{R}} \mathrm{st}(r)$
2) $\mathrm{st}(q \cdot r) = \mathrm{st}(q) \cdot_{\mathbb{R}} \mathrm{st}(r)$
3) ако је $q < r$, онда је $\mathrm{st}(q) \leqslant_{\mathbb{R}} \mathrm{st}(r)$; ако је $\mathrm{st}(q) <_{\mathbb{R}} \mathrm{st}(r)$, онда је $q < r$.

Доказ. Ако су q и r коначни хиперрационални бројеви, онда постоје реални бројеви a и b, и инфинитезимале e и f тако да је $q = a + e$ и $r = b + f$. Према Последици 6, $\mathrm{st}(q) = \mathrm{st}(a) = a$ и $\mathrm{st}(r) = \mathrm{st}(b) = b$.

1) Како је $q + r = a + b + e + f$, а према Леми 22, $e + f$ је инфинитезимала, следи да је $\mathrm{st}(q + r) = \mathrm{st}(a + b) = a +_{\mathbb{R}} b$.

2) Како је $q \cdot r = (a + e) \cdot (b + f) = ab + eb + af + ef$, а према Леми 22, $eb + af + ef$ је инфинитезимала, следи да је $\mathrm{st}(q \cdot r) = \mathrm{st}(a \cdot b) = a \cdot_{\mathbb{R}} b$.

3) Ова својства су једноставне последице дефиниција уређења хиперрационалних и реалних бројева, и дефиниције функције стандардни део. □

Особине доказане у претходној леми преносе особине операција $^*\mathbb{Q}$ на одговарајуће операције над $\mathbb{R}$. Докази су остављени за вежбу.

▼ Компактност

Идеја граничне вредности се препознаје и у многим другим областима. Појам ултрафилтера је посебно користан при проучавању тих феномена. То ћемо показати доказујући једну од најважнијих теорема математичке логике.

Дефиниција 37. *Структура* $\mathbb{M}$ *је модел теорије* Γ, *ако* $\mathbb{M} \models \varphi$, *за свако* $\varphi \in \Gamma$.

Теорема 48. [***Теорема компактности***] *Ако сваки коначан подскуп неке теорије има модел, онда и та теорија има модел.*

Идеја и скица доказа. Доказ спроводимо под претпоставком да је одговарајући вокабулар пребројив, па је самим тим и скуп формула пребројив. Нека је Γ произвољна теорија на таквом вокабулару. Пошто је тада скуп Γ пребројив, све реченице из Γ можемо поређати у низ: $\gamma_0, \gamma_1, \gamma_2, \ldots$. Ако сваки коначан подскуп од Γ има модел, онда за сваки природан број n постоји структура $\mathbf{M}_n$ датог вокабулара таква да $\mathbf{M}_n \models \{\gamma_0, \ldots, \gamma_n\}$. Добијени низ модела $\mathbf{M}_n$, $n \in \mathbb{N}$ можемо схватити као низ све бољих апроксимација траженог модела теорије Γ, јер повећавањем индекса n модели $\mathbf{M}_n$ задовољавају све више реченица теорије Γ. Посебно је важно приметити да свака реченица из Γ важи у скоро свим моделима наведеног низа, тј. у свим осим евентуално у коначно много њих ($\mathbf{M}_n \models \gamma_k$, за $n \geqslant k$, док γ_k не мора важити у моделима $\mathbf{M}_n$ за $n < k$). Заправо, тражени модел теорије Γ биће у одређеном смислу гранична вредност низа модела $\mathbf{M}_n$, $n \in \mathbb{N}$. Очекивано, користимо ултрафилтер $\mathcal{U}$ који проширује Фрешеов филтер.

Модел градимо следећи основне идеје изградње структуре хиперрационалних бројева. Издвајамо само основне кораке, и изостављамо доказе техничких детаља.

Нека је I скуп свих изборних функција за $\{M_n \mid n \in \mathbb{N}\}$, тј. скуп свих низова $f : \mathbb{N} \to \bigcup_{n\in\mathbb{N}} M_n$, таквих да $f(n) \in M_n$, $n \in \mathbb{N}$. На I дефинишемо релацију: $f =_{\mathcal{U}} g \overset{\text{def}}{\Leftrightarrow} (\mathcal{U}n)\,(f(n) = g(n))$.

Релација $=_{\mathcal{U}}$ је релација еквиваленције и класу одређену елементом $f \in I$, означаваћемо $\langle f \rangle$. Нека је M количнички скуп $I/=_{\mathcal{U}}$. Симбол S полазног вокабулара интерпретирамо на скупу M користећи интерпретације тог симбола у структурама $\mathbf{M}_n$:

• ако је c симбол константе, онда је $c^{\mathbf{M}} \overset{\text{def}}{=} \langle c^{\mathbf{M}_n} \rangle$;

• ако је F операцијски симбол дужине k и $\langle f_1 \rangle, \ldots, \langle f_k \rangle \in M$, онда је $F^{\mathbf{M}}(\langle f_1 \rangle, \ldots, \langle f_k \rangle) \overset{\text{def}}{=} \langle F^{\mathbf{M}_n}(f_1(n), \ldots, f_k(n)) \rangle$;

• ако је R релацијски симбол дужине k и $\langle f_1 \rangle, \ldots, \langle f_k \rangle \in M$, онда је $R^{\mathbf{M}}(\langle f_1 \rangle, \ldots, \langle f_k \rangle) \overset{\text{def}}{\Leftrightarrow} (\mathcal{U}n)\, R^{\mathbf{M}_n}(f_1(n), \ldots, f_k(n))$.

Индукцијом по сложености формула доказује се да за сваку формулу $\varphi(x_1, \ldots, x_k)$ и $\langle f_1 \rangle, \ldots, \langle f_k \rangle \in M$:

$$\mathbf{M} \models \varphi(\langle f_1 \rangle, \ldots, \langle f_k \rangle) \Leftrightarrow (\mathcal{U}n)\,(\mathbf{M}_n \models \varphi(f_1(n), \ldots, f_k(n))).$$

Пошто је свака реченица γ из Γ тачна у свим структурама $\mathbf{M}_n$, осим можда у коначно много њих, следи и да $\mathbf{M} \models \gamma$. Дакле, $\mathbf{M}$ је модел теорије Γ. □

Теорема компактности пружа велике могућности примене у различитим областима математике. Поред тога, наведени доказ ове теореме описује и једну веома значајну конструкцију којом се изграђују важне структуре првог реда.

Пример 61. Ако нека теорија T има моделе произвољно велике коначне кардиналности, доказаћемо да тада мора имати и бесконачан модел.

Претпоставимо да је T теорија таква да за свако m постоји модел теорије T чији домен има бар n елемената. Ако је $m > 0$, нека је γ_m реченица $\exists x_1 \cdots \exists x_m \bigwedge_{1 \leqslant i < j \leqslant m} x_i \neq x_j$. Није тешко уочити да реченица γ_m важи у неком моделу акко домен тог модела има бар m елемената. Нека је

$$T^* = T \cup \{\gamma_m \mid m \geqslant 1\}.$$

Доказаћемо да теорија T^* има модел тако што ћемо показати да сваки њен коначан подскуп има модел. Нека је T_0 коначан подскуп од T^*. Тада постоји природан број n такав да је $T_0 \subseteq T_0' = T \cup \{\gamma_1, \ldots, \gamma_n\}$. Теорија T_0' има модел по претпоставци. Ако је $\mathbf{M}$ било који модел теорије T који има најмање n елемената, онда $\mathbf{M} \models \gamma_i$, $1 \leqslant i \leqslant n$, па $\mathbf{M} \models T_0'$, а самим тим и $\mathbf{M} \models T_0$. Према теореми компактности и T^* има модел; означимо га са $\mathbf{M}^*$. Домен овог модела M^* мора бити бесконачан, јер ако би био коначан, онда би било $|M^*| = m$, за неко $m \geqslant 1$, па не би важило $\mathbf{M}^* \models \gamma_{m+1}$.

Претходни пример илуструје како се теорема компактности може искористити да поједине коначне феномене уопштимо на бесконачне. Међутим, она може бити корисна и у обрнутом смеру. Ово ћемо илустровати доказом тзв. коначне верзије Ремзијеве теореме.

Теорема 49. [***Коначна верзија Ремзијеве теореме***] *Нека су $k, r, n \geqslant 1$ произвољни. Постоји природан број $m \geqslant n$, такав да за свако бојење $\pi : m^{[k]} \overset{\text{на}}{\to} r$, k-точланих подскупова од m у r боја, постоји скуп $H \subseteq m$, $|H| = n$, такав да су сви елементи $H^{[k]}$ обојени истом бојом.*

$X^{[k]}$ је скуп свих k-точланих подскупова од X.

Доказ. Претпоставимо супротно, тј. да за свако $m \geqslant n$, постоји бојење $\pi : m^{[k]} \overset{\text{на}}{\to} r$ за које не постоји скуп $H \subseteq m$, $|H| = n$, такав да су сви елементи скупа $H^{[k]}$ обојени истом бојом.

Формираћемо једну теорију вокабулара који садржи r релацијских симбола, $B_1, \ldots, B_r$, од којих су сви дужине k. Интуитивно, $B_i(x_1, \ldots, x_k)$ значи: k-торка $(x_1, \ldots, x_k)$ *је обојена бојом* i. Нека је α конјункција следећих реченица:

$$-\ \forall x_1 \cdots \forall x_k \left(B_i(x_1,\ldots,x_k) \Rightarrow \bigwedge_{1\leqslant i<j\leqslant k} x_i \neq x_j \right),\ 1 \leqslant i \leqslant r,$$

> Речима: обојене су само k-торке међусобно различитих елемената; нису обојене k-торке у којима су бар две координате једнаке.

$$-\ \forall x_1 \cdots \forall x_k \left(B_i(x_1,\ldots,x_k) \Rightarrow \bigwedge_{p\in P_k} B_i(x_{p(1)},\ldots,x_{p(k)}) \right),\ 1 \leqslant i \leqslant r,$$

где је P_k скуп свих пермутација скупа $\{1,\ldots,k\}$,

> Пермутацијом координата не мења се боја k-торке; због ове и претходне особине, бојење k-торки међусобно различитих елемената на јединствен начин одређује бојење k-точланих подскупова.

$$-\ \forall x_1 \cdots \forall x_k \left(\bigwedge_{1\leqslant i<j\leqslant k} x_i \neq x_j \Rightarrow \bigvee_{1\leqslant i\leqslant r} B_i(x_1,\ldots,x_k) \right).$$

> Свака k-торка међусобно различитих елемената обојена је бар једном бојом.

$$-\ \forall x_1 \cdots \forall x_k \left(\bigwedge_{1\leqslant i<j\leqslant k} (\neg B_i(x_1,\ldots,x_k) \vee \neg B_j(x_1,\ldots,x_k)) \right).$$

> Свака k-торка међусобно различитих елемената обојена је највише једном бојом, тј. не може бити обојена двема различитим бојама.

За $i \in \{1,\ldots,r\}$, $\beta_i(x_1,\ldots,x_n)$ је формула $\bigvee_{1\leqslant j_1<\ldots<j_k\leqslant n} B_i(x_{j_1},\ldots,x_{j_k})$.

> Из n-торке $(x_1,\ldots,x_n)$ може се издвојити k-торка $(x_{j_1},\ldots,x_{j_k})$, $1 \leqslant j_1 < \ldots < j_k \leqslant n$, обојена бојом i.

Нека је β реченица $\forall x_1 \cdots \forall x_n \left(\bigwedge_{1\leqslant i<j\leqslant n} x_i \neq x_j \Rightarrow \bigvee_{1\leqslant i<j\leqslant r} (\beta_i(x_1,\ldots,x_n) \wedge \beta_j(x_1,\ldots,x_n)) \right)$.

> Из сваке n-торке међусобно различитих елемената могу се издвојити две k-торке обојене различитим бојама.

Најзад, нека је γ_ℓ, $\ell \geqslant 1$, реченица $\exists x_1 \cdots \exists x_\ell \bigwedge_{1\leqslant i<j\leqslant \ell} x_i \neq x_j$.

> Постоји бар ℓ међусобно различитих елемената.

Докажимо да теорија $T = \{\alpha,\beta,\gamma_1,\gamma_2,\gamma_3,\ldots\}$ има модел. Нека је T_0 произвољан коначан подскуп од T. Тада постоји природан број $m \geqslant n$ такав да је $T_0 \subseteq T_0' = \{\alpha,\beta,\gamma_1,\ldots,\gamma_m\}$. Према нашој полазној претпоставци, постоји бојење $\pi : m^{[k]} \overset{\text{na}}{\to} r$ за које не постоји подскуп $H \subseteq m$, $|H| = n$, чији су k-точлани подскупови обојени истом бојом. За $i \in \{1,\ldots,r\}$, нека $B_i^{\mathbf{m}} \subseteq m^k$ садржи само уређене k-торке међусобно различитих елемената $x_1,\ldots,x_k \in m$ такве да је $\pi(\{x_1,\ldots,x_k\}) = i$. Тада је $(m, B_1^{\mathbf{m}},\ldots,B_r^{\mathbf{m}}) \models T_0'$. Према теореми компактности, и скуп T има модел. Нека је $\mathbf{M} = (M, B_1^{\mathbf{M}},\ldots,B_r^{\mathbf{M}}) \models T$. Приметимо најпре да скуп M мора би-

ти бесконачан. Дефинишимо функцију $\pi : M^{[k]} \to r$ на следећи начин:

$$\pi(\{x_1, \dots, x_k\}) = i \overset{\text{def}}{\Leftrightarrow} B_i^{\mathbf{M}}(x_1, \dots, x_k), \text{ за међусобно различите } x_1, \dots, x_k \in M.$$

Према бесконачној варијанти Ремзијеве теореме постоји бесконачан скуп $H \subseteq M$ чији су k-точлани подскупови обојени истом бојом. Свакако из овог скупа можемо издвојити n међусобно различитих елемената $h_1, \dots, h_n$ од којих се не могу формирати два скупа са по k елемената који ће бити различитих боја, што противречи чињеници да $\mathbf{M} \models \beta$. □

▼ Задаци и додаци

1. Доказати, за произвољне $x, y, z \in \mathbb{R}$:

$x +_{\mathbb{R}} (y +_{\mathbb{R}} z) = (x +_{\mathbb{R}} y) +_{\mathbb{R}} z$	$x \cdot_{\mathbb{R}} (y \cdot_{\mathbb{R}} z) = (x \cdot_{\mathbb{R}} y) \cdot_{\mathbb{R}} z$
$x +_{\mathbb{R}} y = y +_{\mathbb{R}} x$	$x \cdot_{\mathbb{R}} y = y \cdot_{\mathbb{R}} x$
$x +_{\mathbb{R}} 0 = x$	$x \cdot_{\mathbb{R}} 1 = x,\ x \cdot_{\mathbb{R}} 0 = 0$
$(\exists u \in \mathbb{R})(x +_{\mathbb{R}} u = 0)$	$x \cdot_{\mathbb{R}} (y +_{\mathbb{R}} z) = x \cdot_{\mathbb{R}} y +_{\mathbb{R}} x \cdot_{\mathbb{R}} z$

$$(*)\quad x \neq 0 \Rightarrow (\exists u \in \mathbb{R})\, x \cdot_{\mathbb{R}} u = 1$$

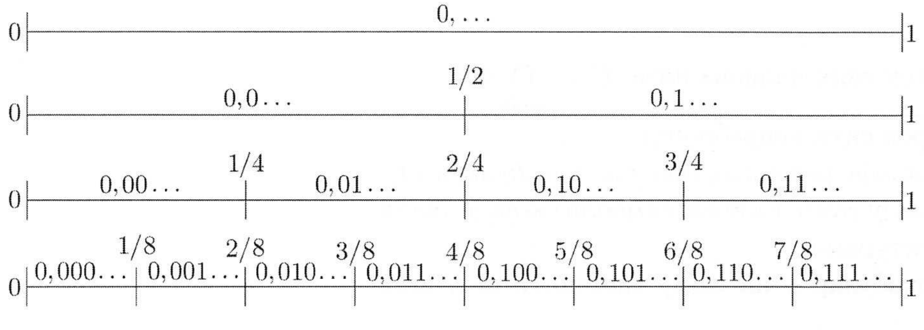
$x \leqslant_{\mathbb{R}} x$	$x \leqslant_{\mathbb{R}} y \wedge y \leqslant_{\mathbb{R}} x \Rightarrow x = y$
$x \leqslant_{\mathbb{R}} y \wedge y \leqslant_{\mathbb{R}} z \Rightarrow x \leqslant_{\mathbb{R}} z$	$x \leqslant_{\mathbb{R}} y \vee y \leqslant_{\mathbb{R}} x$
$x \leqslant_{\mathbb{R}} y \Rightarrow x +_{\mathbb{R}} z \leqslant_{\mathbb{R}} y +_{\mathbb{R}} z$	$x \leqslant_{\mathbb{R}} y \wedge 0 \leqslant_{\mathbb{R}} z \Rightarrow x \cdot_{\mathbb{R}} z \leqslant_{\mathbb{R}} y \cdot_{\mathbb{R}} z$

2. Испитати тачност следећих реченица у структурама (истог вокабулара) $\mathbf{Q} = (\mathbb{Q}, \leqslant, +, \cdot, -, 0, 1)$ и $\mathbf{R} = (\mathbb{R}, \leqslant, +, \cdot, -, 0, 1)$:

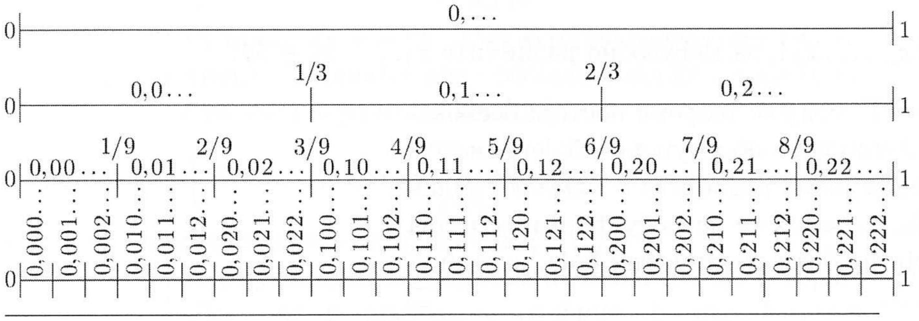
(а) $\forall a \forall b \exists x\, (a \cdot x = b)$
(б) $\forall a \forall b (a \neq 0 \Rightarrow \exists x\, (a \cdot x = b))$
(в) $\forall a \forall b \exists x\, (x \cdot x + a \cdot x + b = 0)$
(г) $\forall a \exists x\, (x \cdot x + a \cdot x = 0)$
(д) $\forall a \forall b \exists x\, (x \cdot x + a \cdot b = (a + b) \cdot x)$
(ђ) $\forall a \forall b ((b + b) + (b + b) \leqslant a \cdot a \Rightarrow \exists x\, (x \cdot x + a \cdot x + b = 0))$
(е) $\forall a \forall b \exists c \forall x\, (c \leqslant x \cdot x + a \cdot x + b)$

Додатак

Аналогно децималним записима, реалне бројеве можемо репрезентовати и у другим системима: бинарним, тернарним итд. Слободно говорећи, основу система одређује договор на колико делова делимо јединицу мере. У децималном систему, јединицу мере уситњавамо узастопним поделама на 10 једнаких делова. У бинарном систему, јединицу мере уситњавамо поделама на 2 једнака дела, а децимале записујемо цифрама 0 и 1:



У систему са основом 3, дужи којима меримо делимо на три дела, и сходно томе, децималне бројеве записујемо цифрама 0, 1 и 2:



3. Доказати да је скуп реалних бројева непребројив. [191]

4. Доказати да је:

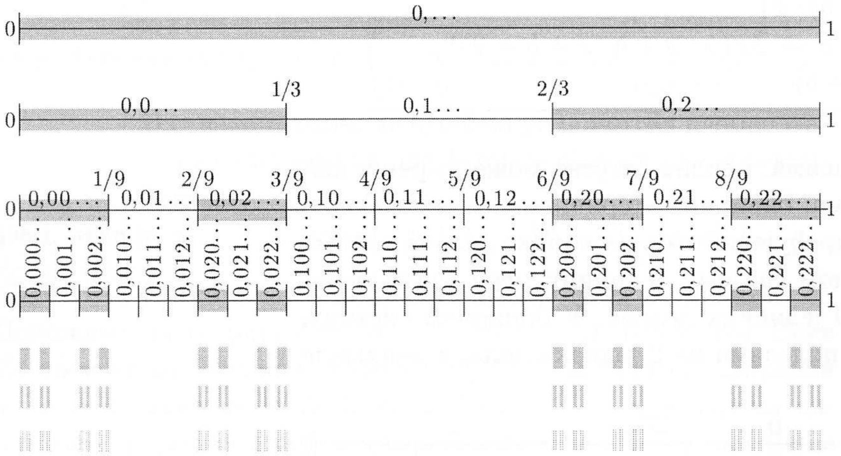
(а) $|\mathbb{R}| = |\mathbb{R} \times \mathbb{R}|$; (б) $|\mathbb{R}| = |\mathbb{R}^{\mathbb{N}}|$.

Додатак

Канторов скуп се добија од јединичног интервала $[0,1]$ узастопним брисањем средњег отвореног интервала. Полазећи од $[0,1]$, најпре се брише отворени интервал $\left(\frac{1}{3},\frac{2}{3}\right)$, након чега остаје $\left[0,\frac{1}{3}\right] \cup \left[\frac{2}{3},1\right]$. Затим, се из сваког од добијених интервала изоставља средњи отворени интервал и остаје $\left[0,\frac{1}{9}\right] \cup \left[\frac{2}{9},\frac{1}{3}\right] \cup \left[\frac{2}{3},\frac{7}{9}\right] \cup \left[\frac{8}{9},1\right]$. Поново се из сваког интервала изоставља средњи отворени интервал итд. Добијени низ скупова је индуктивно дефинисан следећим једнакостима:

$$C_0 = [0,1]$$
$$C_{n+1} = \frac{C_n}{3} \cup \left(\frac{2}{3} + \frac{C_n}{3}\right), n \geqslant 0$$

Ако је $X \subseteq \mathbb{R}$, онда је:
$\frac{X}{3} \overset{\text{def}}{=} \{\frac{x}{3} \mid x \in X\}$
$\frac{2}{3} + \frac{X}{3} \overset{\text{def}}{=} \{\frac{2}{3} + \frac{x}{3} \mid x \in X\}$



Канторов скуп је пресек свих чланова низа: $C = \bigcap_{n \in \mathbb{N}} C_n$.

---

5. Доказати да је Канторов скуп непребројив.

6. (а) Доказати да не постоји реченица празног вокабулара (тј. реченица у којој се појављују само логички симболи) која је тачна само у бесконачним структурама.

(б) Погодно изабрати вокабулар и на њему саставити реченицу

[191] Довољно је доказати да је непребројив неки подскуп скупа $\mathbb{R}$. На пример, $[0,1)$. Корисно је приметити кореспонденцију између децималних развоја у бинарном систему $0,d_1d_2d_3\ldots$ и бинарних низова (без низа свих јединица).

која је тачна само у бесконачним структурама.

7. [193] Нека је σ L-реченица. Ако је σ тачна у свим коначним L-структурама, доказати да је тачна и у некој бесконачној L-структури.

Упутство. Применом теореме компактности доказати да следећа теорија има модел: $T = \{\sigma, \gamma_1, \gamma_2, \gamma_3, \ldots\}$, где су γ_m, $m \geqslant 1$, реченице из Примера 61 (страна 171).

8. Нека је Γ скуп L-реченица и σ нека L-реченица. Доказати:
(а) $\Gamma \cup \{\neg\sigma\}$ има модел акко $\Gamma \not\models \sigma$;
(б) ако $\Gamma \models \sigma$, онда постоји коначан подскуп $\Gamma_0 \subseteq \Gamma$ такав да $\Gamma_0 \models \sigma$.

9. Нека је Γ скуп L-реченица. Испитати да ли је тачно следеће тврђење: Скуп Γ има контрамодел акко сваки коначан подскуп од Γ има контрамодел.

Напомена. Контрамодел скупа Γ формула јесте L-структура у којој нису тачне све формуле датог скупа. Другим речима, за сваку L-структуру постоји реченица из Γ која није тачна у тој структури.

10. Нека је Γ скуп L-реченица такав да свака L-структура задовољава бар једну реченицу из Γ. Доказати да постоји коначан подскуп $\{\gamma_1, \ldots, \gamma_m\} \subseteq \Gamma$ такав да је $\gamma_1 \vee \cdots \vee \gamma_m$ ваљана формула.

[193] „Формулу вокабулара L" краће називамо „L-формула". Слично томе, „структуру вокабулара L" краће називамо „L-структура".

Литература

1. S.N. Burris, K.A. Yeats, *The saga of the High School Identities*, Algebra universalis, 52, 325–342, 2005

2. R. David, K. Nour, C. Raffali, *Introduction à la logique – Théorie de la démonstration*, Dunod, Paris, 2003

3. R. Kaye, *The Mathematics of Logic – a guide of completeness theorems and their applications*, Cambridge University Press, 2007

4. М. Курилић, *Основи опште топологије*, Универзитет у Новом Саду, Природно-математички факултет, Нови Сад, 1998

5. И. А. Лавров, Л. Л. Максимова, *Задачи по теории множеств, математической логике и теории алгоритмов*, Наука, Москва, 1984.

6. J. Lewin, *A Simple Proof of Zorn's Lemma*, The American Mathematical Monthly, 98:4, 353-354, 1991

7. З. Петровић, Ж Мијајловић, *Математичка логика – елементи теорије скупова*, Завод за уџбенике, Београд, 2012

8. С. Прешић, *Елементи математичке логике*, Завод за издавање уџбеника, Београд, 1968

9. М. Рашковић, Н. Икодиновић, *Приче о малим и великим бројевима – о бројању, мерењу, закључивању ...*, МИ САНУ, Завод за уџбенике, ДМС, Београд, 2010

10. S. Todorčević, *Introduction to Ramsey spaces*, Annals of Mathematics Studies, vol. 174, Princeton University Press, 2010

11. S. Hedman, *A First Course in Logic – an Introduction to Model Theory, Proof Theory, Computability and Complexity*, Oxfor University Press, 2006

Предлози за читање [194]

- M. Božić, A. Ivić, A. Jovanović, M. Kapetanović, M. Mihaljinec, Ž Mojajlović, S. Prešić, M. Prešić, M. Rašković, D. Rosenzweig, Z. Šami, K. Šeper, Z. Šikić, D. Ugrin-Šparac, *Brojevi*, Školska knjiga, Zagreb, 1985

- S. Vujošević, *Matematička logika – o mogućnostima formalnog metoda*, CID, Podgorica, 1996
`http://elibrary.matf.bg.ac.rs/handle/123456789/2492`

- M. Davis, *Na logički pogon – podrijetlo ideje računala*, Naklada Jesenski i Turk, Zagreb, 2003

[194] Поред референци које су коришћене приликом писања ове књиге, препоручујемо још неколико домаћих издања и превода. Поједини наслови су доступни у Виртуелној библиотеци Математичког факултета. `elibrary.matf.bg.ac.rs`

- P. Janičić, *Matematička logika u računarstvu*, Matematički fakultet, Beograd, 2005
`http://www.matf.bg.ac.rs/~janicic/books/mlr.pdf`
- M. Kac, S. Ulam, *Matematika i logika – retrospektiva i perspektive*, Školska knjiga, Zagreb, 1977
- Ž. Mijajlović, Z. Marković, K. Došen, *Hilbertovi problemi i logika*, Zavod za udžbenike i nastavna sredstva, Beograd, 1986.
`http://elibrary.matf.bg.ac.rs/handle/123456789/593`
- Ž. Mijajlović, *Algebra 1*, Milgor, Beograd–Moskva 1993.
`http://elibrary.matf.bg.ac.rs/handle/123456789/462`
- Ж. Мијајловић, М. Рашковић, Д. Аранђеловић, Р. Ђорђевић, *Нестандардна анализа*, Математички факултет, Београд, 2014
`http://elibrary.matf.bg.ac.rs/handle/123456789/5429`
- A. Perović, A. Jovanović, B. Veličković, *Teorija skupova – matematička teorija beskonačnosti*, 2007
`http://elibrary.matf.bg.ac.rs/handle/123456789/473`
- Z. Šikić, *Kako je stvarana novovjekovna matematika*, Školska knjiga, Zagreb, 1989
`http://elibrary.matf.bg.ac.rs/handle/123456789/5569`

Индекс

аксиома
  бесконачности, 118
  екстензионалности, 87
  избора, 136
  пара, 89
  партитивног скупа, 89
  празног скупа, 88
  регуларности, 117
  уније, 89
алфабет, 36
бинарна операција, 107
бинарна релација, 97
  антисиметрична, 103
  домен, 98
  инверзна релација, 101
  ирефлексивна, 103
  кодомен, 98
  композиција релација, 99
  линеарна, 103
  празна релација, 97
  пуна релација, 97
  релација еквиваленције, 103
  релација поретка, 105
  рефлексивна, 103
  симетрична, 103
  транзитивна, 103
валуација
  атомских реченица, 70
  исказних слова, 12
  променљивих, 70
Декартов
  производ, 95
  степен, 96
дијагонала скупа, 98
дисјунктни скупови, 93
децимални развој, 165
еквивалентне формуле, 19
елиминација
  дисјункције, 63
  $\exists$ квантификатора, 79
  еквиваленције, 62
  импликације, 61
  конјункције, 61
  негације, 62
  $\forall$ квантификатора, 78
задовољива формула, 13
извођење
  из хипотеза у формалној теорији, 41
  у формалној теорији, 40
инклузија, 88
исказна алгебра, 9
исказна формула, 10
  инстанца, 18
језик
  одређен граматиком, 37
  првог реда, 149
    атомске формуле, 150
    ваљана формула, 153
    вокабулар структуре, 149
    вредност израза, 151
    истинитосна вредност формуле, 151
    изрази, 150
    тачност реченице, 152
    теорема потпуности, 156
    теорема сагласности, 156
    формуле, 150
  чист предикатски, 69
    атомска формула, 69
    предикатска формула, 70
    реченица, 70

класа еквиваленције, 104
количнички скуп, 104
комплемент подскупа, 93
квантификатор $\mathcal{U}$-скоро сви, 142
лема
  Тарски, 131
  Цермело, 139
  Цорн, 137
логичке операције, 9
модел теорије, 170
нормална форма
  дисјунктивна, 21
  конјунктивна, 21
партиција скупа, 114
правило класичне непротивречности, 62
пресек
  два скупа, 93
  скупа, 91
принцип
  Дирихлеов, 129
  математичке индукције, 28, 119
  математичке индукције са две хипотезе, 31
  потпуне математичке индукције, 31, 121
рачун Ł, 49
  теорема дедукције, 50
  теорема потпуности, 55
  теорема сагласности, 50
разлика два скупа, 93
реч, 36
секвент, 63
семантичка последица, 153
синтаксна последица, 154
скуп
  бесконачан, 130
  индуктиван, 118
  Канторов, 174
  кардиналност, 130
  коначан, 129
  највише пребројив, 133
  непребројив, 133
  пребројив, 133
  природних бројева, 119
  рационалних бројева, 147
  реалних бројева, 168
следбеник скупа, 117
слободна променљива, 70
схема
  замене, 117
  издвајања, 89
таутологија, 13
  закон двојне негације, 14
  закон искључења трећег, 14
  закон контрапозиције, 14
  модус поненс, 14
  модус толенс, 14
  свођење на противречност, 14
  транзитивност импликације, 14
теорема
  Кантор-Бернштајнова, 131
  компактности, 170
  предикатског рачуна, 80
  рекурзије, 122
  Ремзијева, 143, 171
  формалне теорије, 40
теорија, 152
  група, 161
  уређених група, 152
унија два скупа, 93
уређен пар, 94
уређена тројка, 96
уређење, 105
  добро, 122, 135
  лексикографско, 114
  линеарно, 105
  максимални елемент, 106
  минимални елемент, 106
  највећи елемент, 106
  најмањи елемент, 106
  строго, 105
увођење
  дисјункције, 62
  $\exists$ квантификатора, 78
  еквиваленције, 62
  импликације, 61
  конјункције, 61
  негације, 62
  $\forall$ квантификатора, 79
фамилија скупова, 115
филтер, 140
  ултрафилтер, 141
  Фрешеов филтер, 140

формална
  граматика, 37
  теорија, 40
функција, 98
  бијекција, 102
  директна слика, 108
  ињекција (1-1 функција), 102
  идентичка, 99
  индиректна слика, 108
  карактеристична, 107
  рестрикција, 106
  сирјекција (на функција), 102
хиперрационалан број, 165

Белешке:

Током људске историје, исказ

Земља се окреће око Сунца

некада је сматран нетачним, а некада тачним. Без обзира на то, увек се знало да је тачан исказ:

Земља се окреће око Сунца
или
Земља се не окреће око Сунца.

ISBN 978-86-7589-177-2